NORMAN

Norman Virus Control per workstation

Versione 5.81

Guida di riferimento

Garanzia limitata

Norman garantisce che il dischetto/CD-ROM e la documentazione inclusi nella confezione non presentano difetti di produzione. Nel caso in cui rileviate un difetto entro 30 giorni dalla data di acquisto, Norman sostituirà gratuitamente la documentazione e/o il dischetto/CD-ROM difettosi. Assieme ad ogni reclamo deve essere allegata una prova di acquisto del prodotto.

La presente garanzia è limitata alla sostituzione del prodotto. Norman non è responsabile di altre forme di perdita o danno risultanti dall'uso del software o della documentazione, né da relativi errori o difetti, incluso ma non limitatamente alla perdita di profitti.

Relativamente a difetti o anomalie del dischetto/CD-ROM, o della documentazione, o di questo accordo di licenza, la presente garanzia sostituisce ogni altra garanzia, esplicita o implicita, incluso ma non limitatamente a garanzie implicite di commerciabilità e idoneità per scopi particolari.

In particolare, e senza le limitazioni imposte dal contratto di licenza relativamente a qualsiasi uso o scopo specifico, Norman non sarà in alcun modo responsabile della perdita di profitti né di altri danni commerciali compresi, incluso ma non limitatamente a danni accidentali o indiretti.

La presente garanzia scade 30 giorni dopo la data di acquisto.

Le informazioni presenti in questo documento, così come la funzionalità del software, sono soggette a modifica senza preavviso. Il software può essere utilizzato secondo i termini del contratto di licenza. L'acquirente può eseguire una copia del software a scopo di backup. Nessuna parte di questa documentazione può essere riprodotta o trasmessa in alcuna forma e in alcun modo, elettronico o meccanico, comprese fotocopie, registrazione di informazioni e sistemi di recupero dati, per scopi diversi dall'uso personale dell'utente, senza espressa autorizzazione scritta di Norman.

Il logo Norman è un marchio registrato della Norman ASA.

I nomi dei prodotti citati in questo documento sono marchi di fabbrica o marchi registrati dei rispettivi proprietari e vengono citati esclusivamente a scopo di identificazione.

La documentazione e il software NVC sono

Copyright © 1990-2005 Norman ASA.

Tutti i diritti riservati.

Ultima revisione 9 giugno 2005.

Sedi Norman

Norman Data Defense Systems AS
Blangstedgårdsvej 1, DK-Odense SØ, **Danimarca**
Tel. +45 6311 0508 Fax: +45 6313 3901
E-mail: normandk@normandk.com Sito Web: http://www.norman.no/dk

Norman Ibas OY
Läkkisepäntie 11, 00620 Helsinki, **Finlandia**.
Tel: +358 9 2727 210 Fax: +358 92727 2121
E-mail: norman@norman-ibas.fi Sito Web: http://www.norman-ibas.fi

Norman Data Defense Systems GmbH
Gladbecker Str. 3, D-40472 Düsseldorf, **Germania**.
Tel: +49.211.586 99 -0 Fax: +49 211 586 99-150
E-mail: norman@norman.de Sito Web: http://www.norman.de

Norman/SHARK BV
Postbus 159, 2130 AD, Hoofddorp, **Paesi Bassi**.
Tel: +31 23 789 02 22 Fax: +31 23 561 3165
E-mail: support@norman.nl Sito Web: http://www.norman.nl

Norman ASA
Indirizzo: P.O. Box 43, N-1324, Lysaker, **Norvegia**.
Indirizzo: Strandveien 37, Lysaker, N-1324 Norvegia.
Tel: +47 67 10 97 00 Fax: +47 67 58 99 40
E-mail: norman@norman.no Sito Web: http://www.norman.no/no

Norman Data Defense Systems AB
S.t Persgatan 19, SE-601 86 Norrköping, **Svezia**
Tel. +46 11 230 330 Fax: +4611 230 349
E-mail: support.se@norman.no Sito web: http://www.norman.com/se

Norman Data Defense Systems AG
Postfach CH-4015, Basilea, **Svizzera**.
Tel: +41 61 487 2500 Fax: +41 8 87 52 52
E-mail: norman@norman.ch Sito Web: http://www.norman.ch

Norman Data Defense Systems (UK) Ltd
Unit 15, Linford Forum, Rockingham Drive, Linford Wood,
Milton Keynes, MK14 6LYPO, **Regno Unito**.
Tel: +44 08707 448044 Fax: +44 08717 176999
E-mail: norman@normanuk.com Sito Web: http://www.normanuk.com

Norman Data Defense Systems Inc.
9302 Lee Highway, Suite 950A, Fairfax, VA 22031, **USA**
Tel: +1 703 267 6109, Fax: +1 703 934 6367
E-mail: norman@norman.com Sito Web: http://www.norman.com

Addestramento e assistenza tecnica

Per l'addestramento o l'assistenza tecnica rivolgersi al rivenditore locale oppure alla Norman ASA.

Copyright © 1990-2005 Norman

Convenzioni

I paragrafi riservati agli utenti di una rete o all'amministratore della rete, e che pertanto non interessano gli utenti singoli, sono contrassegnati dall'icona di una rete posta sul margine sinistro della pagina.

Questo manuale è destinato agli utenti Windows e OS/2. In caso di differenze specifiche per una piattaforma, questa icona posta sul margine della pagina segnala una procedura speciale per OS/2.

Requisiti di sistema

È possibile installare NVC v5 su
Windows 95/98/Me, Windows NT/2000/XP/2003, Linux, OS/2 Warp 4, OS/2 Warp Server, Workspace On-demand e eComStation.

Per Windows 95 è necessario installare WinSock2 e si consiglia di utilizzare Internet Explorer 5.5.

Per Windows NT sono necessarie la versione 4 con SP4 (o successiva) e Internet Explorer 4.0 (o successiva).

Per OS/2 si consiglia Warp 4 fp 15 (o versione successiva) e Java 1.1.8.

Per Linux è necessario utilizzare glibc 2.2.

In generale, si consiglia di utilizzare gli ultimi aggiornamenti di service pack e relativi alla sicurezza per la piattaforma in uso.

Copyright © 1990-2005 Norman

Destinatari del manuale

Il presente manuale illustra tutte le funzioni di NVC e pertanto è destinato a tutti gli utenti di NVC, utenti singoli come pure amministratori, che desiderano avere informazioni dettagliate su questo prodotto.

Oltre a questo manuale, il *Manuale dell'amministratore* approfondisce gli argomenti particolarmente utili per i responsabili delle installazioni in ambienti di rete, mentre il *Manuale dell'utente* offre una breve presentazione delle funzioni di base di NVC.

In questo manuale *non* è illustrata l'installazione di NVC. Per l'installazione in rete e su macchine autonome consultare rispettivamente il *Manuale dell'amministratore* e il *Manuale dell'utente*.

Prerequisiti

Per sfruttare al massimo tutte le funzioni di NVC, sarebbe opportuno avere una buona conoscenza dei diversi moduli di NVC e di come interagiscono tra loro, come descritto nel presente manuale.

Se si esegue NVC in una rete, è opportuno avere conoscenze dettagliate del sistema operativo o dei sistemi operativi presenti sui server e sulle workstation come pure dell'installazione della rete.

Supporto tecnico

La Norman fornisce assistenza tecnica e servizi di consulenza per l'utilizzo di NVC e in generale per problematiche relative alla sicurezza. L'assistenza tecnica offre anche l'assicurazione della qualità dell'installazione dell'antivirus, compreso la consulenza per personalizzare NVC in base ad esigenze specifiche.

La quantità di servizi disponibili può variare da paese a paese.

Copyright © 1990-2005 Norman

Copyright © 1990-2005 Norman

Sommario

Convenzioni iv
Requisiti di sistema iv
Destinatari del manuale v
Supporto tecnico v

Informazioni generali su NVC 11

Cos'è NVC? 11
Informazioni generali su NVC 5 11

Programmi e moduli NVC 13

Panoramica di NVC 14
Collegamento ai moduli NVC e alla scansione 14
Editor di Configurazione 17

Installazione e aggiornamento dei prodotti 19

Installazione 19
Aggiornamento di NVC 20
LAN/WAN 21
Internet 26
Server proxy 29

Norman Program Manager 32

Componenti 33
Installazione 33
Informazioni su messaggistica e log 33
Gestione messaggi 33
Logger messaggi 35
Console messaggi 37

Copyright © 1990-2005 Norman

Registro eventi 38
Messaggio definito dall'utente 38
Routing messaggi..... 40
Messaggi 40
Routing 41
E-mail, SMS, SNMP..... 42
Messaggi per E-mail, SMS e SNMP 42
Configura messaggi e-mail 44
Configura messaggi SMS 46
Configura SNMP 48

Norman Virus Control 50

Componenti..... 50
Installa 50
Avvio 52
Impostazioni comuni..... 53
Lista di esclusione 53
Scansione su richiesta 54
Scansione 55
file di log 59
File d'archivio 61
File infetti negli archivi 61
Scansione attivata mediante il pulsante destro del mouse 62
Diagnosi 62
Scansione all'accesso 63
Scansione all'accesso in Windows NT/2000/XP/2003 63
Informazioni sulla Scansione all'accesso in Windows 95/98/Me 64
Scansione 65
Pulizia 71
Scansione all'accesso nelle reti 72
Norman Internet Protection..... 73
Definizioni 74
Lettori di news 74
Winsock 74
Protocollo 74
Porta 75
Come funziona 76

Copyright © 1990-2005 Norman

Attivazione di NIP 77
Scansione dei virus 78
Sostituzione del contenuto nei messaggi di posta elettronica 78
Configurazione del NIP 79
Scansione 79
Blocco degli allegati 81
Avanzate 85

Norman Quarantine 87

Quarantena 87

NVC sui Terminal Server di Windows 89

Editor Operazioni 91

Generale 92
Target 92
Selezione dei target 93
Opzioni di scansione comuni 94
Opzioni 95
Programma 96
Informazioni sul pianificatore..... 97

Utilità 98

File Operazione..... 98
Quarantena 100
Messaggi 101
Scheda Messaggi 101
Scheda File di messaggio 103

Aggiornamento di NVC 104

Norman Internet Update 104
Avvio di Internet Update 104
Internet Update e connessione Internet..... 105
Funzionamento di Internet Update 106
LAN/WAN 107

Copyright © 1990-2005 Norman

Informazioni varie su NVC 108

Norman Program Manager (NPM) 108
Informazioni sulla scansione da linea di comando 109
Avvio della scansione da riga di comando 109
Pulizia dei file infetti..... 110
Esecuzione dei file Operazione dalla linea di comando 111
Opzioni della scansione da linea di comando 111
Abbinamento dei diversi parametri 114
Livelli di errore della scansione da linea di comando 115

Appendice A - Sandbox 117

Premessa 117
Cos'è un "sandbox"? 117
Tecniche di sicurezza con Sandbox 118
Quali sono i vantaggi per l'utente? 118
Cosa fare quando Sandbox rileva un nuovo virus 119

Domande frequenti (FAQ) 121

Indice 125

Copyright © 1990-2005 Norman

Informazioni generali su NVC

Cos'è NVC?

Norman Virus Control (NVC) è un programma antivirus che controlla l'eventuale presenza sul PC di codice dannoso, chiamato anche *malware*. Per codice dannoso si intendono virus, worm e altri tipi di codice in grado di distruggere le risorse. NVC è in grado di rilevare e rimuove virus noti e sconosciuti dai dischi rigidi, dai dischetti, dagli allegati di posta elettronica, ecc.

NVC controlla i file nel momento in cui vi si accede e rimuove automaticamente gli eventuali virus. Se NVC non è in grado di pulire in file infetto, visualizza un messaggio e le istruzioni per come procedere.

È possibile, e consigliabile, eseguire delle scansioni manuali di aree selezionate del computer e utilizzare l'editor e il pianificatore Operazioni per definire cosa analizzare e quando.

Nota: Le impostazioni predefinite di NVC sono sufficienti per proteggere dagli attacchi dei virus. La maggior parte dei moduli sono configurabili per adattare NVC alle proprie esigenze.

Informazioni generali su NVC 5

NVC v5 utilizza due meccanismi di rete diversi:

- Per l'installazione, la distribuzione e la configurazione utilizza la normale condivisione dei file con le lettere delle unità o i percorsi UNC.
- Per i messaggi e i log è stato ideato un livello di protocollo di rete proprietario.

Il sistema di messaggistica fa parte dell'installazione di base di NVC su un computer in rete ed è attivo non appena viene eseguito l'agente residente che, tra l'altro, gestisce il traffico tra i diversi moduli di input e output. L'amministratore deve semplicemente configurare il sistema in modo tale che i

Copyright © 1990-2005 Norman

messaggi di varia importanza vengano passati ai diversi moduli di output dei messaggi.

Il motore di scansione ora utilizza le istruzioni FPU (Floating Point Unit) e MMX (Multi Media Extensions) per rilevare e rimuovere i virus. Anche se ad oggi solo un paio di virus utilizzano le istruzioni FPU o MMX, il loro numero crescerà.

L’emulatore a 32 bit del motore di scansione consente il rilevamento e l'analisi di virus complessi, crittografati e polimorfici.

Qui di seguito sono riassunte alcune delle modifiche più importanti apportate a NVC v5:

- Installazione semplificata
- Gestione semplificata
- Facilità di utilizzo
- Invisibilità

L'interfaccia utente di NVC v5 è suddivisa in quattro gruppi principali:

- Editor di Configurazione
- Editor Operazioni
- Utilità
- Internet Update

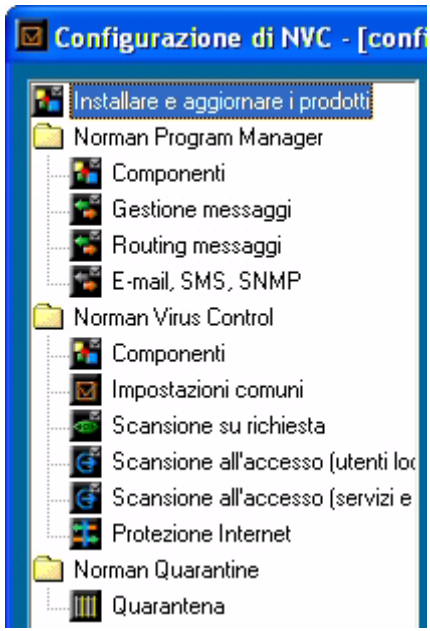
Sono visualizzati come voci distinte nel gruppo di programmi Norman.

Questi gruppi si trovano nella cartella Norman del desktop di OS/2.

⇨ Consultare i capitoli ‘Editor di Configurazione' a pagina 17, ‘Editor Operazioni' a pagina 91, ‘Utilità' a pagina 98 e ‘Norman Internet Update' a pagina 104.

Copyright © 1990-2005 Norman

Programmi e moduli NVC



In questo capitolo viene descritta la presentazione di NVC e altri prodotti Norman nell'Editor di Configurazione. Sul lato sinistro dell'Editor viene visualizzato un elenco di prodotti e moduli/componenti. Nell'elenco vengono visualizzati i prodotti Norman installati e i componenti e i moduli corrispondenti per ciascun programma sono organizzati sotto forma di *cartelle* con la stessa logica e lo stesso aspetto dell'ambiente Esplora risorse di Windows. I moduli sono costituiti da una o più finestre di dialogo con schede in cui sono disponibili le opzioni di configurazione.

La prima voce dell'esempio precedente, **Installazione e aggiornamento dei prodotti**, riguarda l'installazione dei prodotti Norman abilitati per l'esecuzione in questo ambiente e la relativa manutenzione, in particolare la funzionalità Internet Update. Quando si seleziona una delle voci a sinistra, le opzioni di configurazione per il modulo selezionato vengono visualizzate nel lato destro della finestra di dialogo.

Norman Program Manager incorpora moduli che possono essere condivisi da diversi programmi o plug-in Norman pronti per essere inclusi in questa interfaccia utente. I moduli in questa cartella sono controllati da ***Zanda*** (Zero Administration Network Distribution Agent).

⇨ ‘Norman Program Manager (NPM)' a pagina 108.

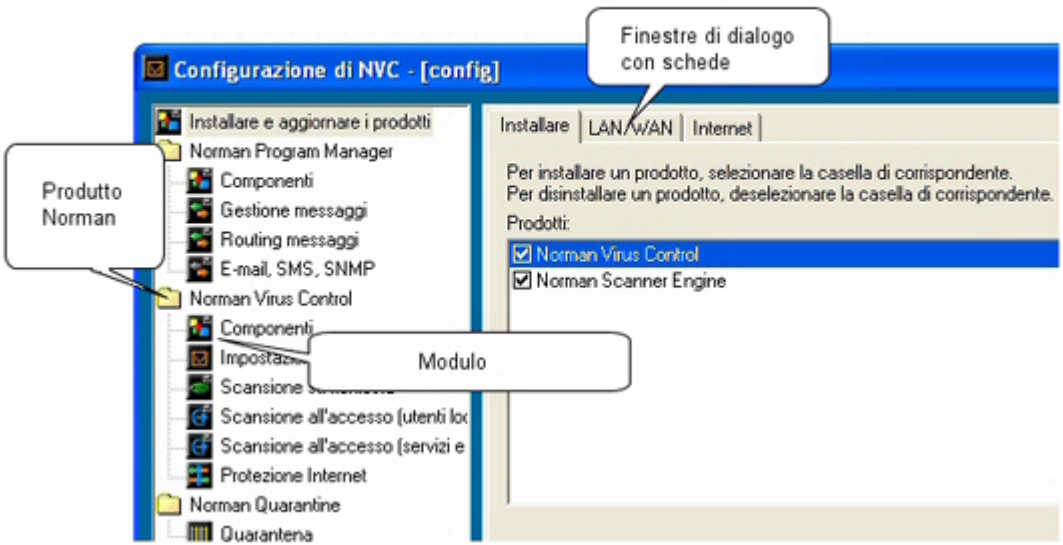
I moduli specifici del prodotto sono elencati sotto **Norman Virus Control**. Selezionare **Componenti** per visualizzare un

Copyright © 1990-2005 Norman

elenco dei componenti di NVC. È possibile installare e rimuovere i componenti da questa finestra di dialogo con schede.

Panoramica di NVC

Come descritto nella sezione precedente, l'interfaccia utente per NVC v5.8 ha il seguente aspetto:



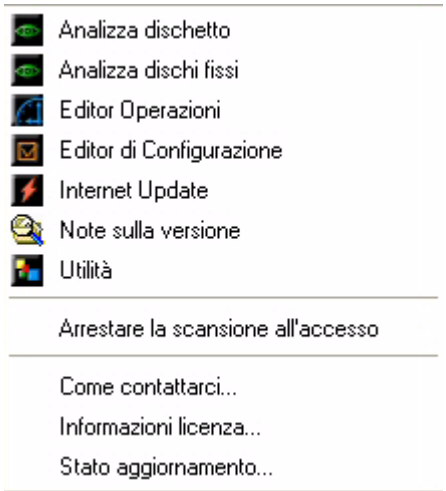
Collegamento ai moduli NVC e alla scansione

Durante l'installazione viene inserita l'icona di Norman nella barra delle applicazioni, nell'angolo in basso a destra dello schermo. Questa icona conferma che NVC è installato sul computer. Vedere pagina 15.

OS/2: NVC viene visualizzato come voce del menu nel desktop. Fare clic con il pulsante destro del mouse sul desktop e selezionare *Norman Virus Control*.

Le voci elencate al di sopra della linea di separazione del menu, che vengono visualizzate quando si sceglie questa icona, sono delle copie delle voci visualizzate in qualsiasi momento nel menu Start|Programmi|Norman Virus Control.

Copyright © 1990-2005 Norman



Questo menu di scelta rapida consente di accedere ai moduli principali di NVC e ad alcune operazioni di scansione di NVC. In Windows è possibile fare clic su uno dei due pulsanti del mouse per visualizzarlo. Questo menu consente di accedere facilmente ai moduli e alle attività di scansione NVC. È possibile **avviare/interrompere la scansione all'accesso** con un semplice clic del mouse. Selezionare **Contatti** per visualizzare le informazioni su come contattare sedi e distributori sul sito Web di Norman o visualizzare la licenza. Infine, è possibile visualizzare lo stato di aggiornamento per i prodotti Norman, incluse informazioni chiave sui file di definizione dei virus.

Inoltre questa funzione consente di visualizzare messaggi relativi ai file di definizione dei virus scaduti e alla scadenza della licenza ed altre informazioni.

Messaggi di avvertimento

L'icona di Norman fornisce anche informazioni sullo stato dell'installazione di NVC. Se l'icona viene visualizzata in questo modo:

indica che i componenti di NVC in esecuzione non corrispondono a quelli selezionati nella scheda **Avvio** del percorso **Norman Virus Control|Componenti|Avvio** nell'Editor di Configurazione. Se la 'N' di Norman viene visualizzata con il simbolo rosso lampeggiante, quando si posiziona il puntatore sul simbolo NVC indica quale componente è necessario aggiornare o segnala eventuali situazioni di errore.

Copyright © 1990-2005 Norman

Nota: Il simbolo rosso è visibile all'avvio fino a quando non sono stati avviati tutti i moduli. Più è lenta la macchina, più tempo occorre per caricare tutti i moduli. Il simbolo "normale" dovrebbe comunque apparire dopo circa 1-2 minuti.

Per gli utenti di Windows XP che hanno installato SP2:
Microsoft ha incluso il "Centro sicurezza" con opzioni e funzioni per firewall, aggiornamenti automatici e protezione da virus. NVC è uno dei fornitori di antivirus rilevati dal sistema operativo. Se i file di definizione dei virus di NVC sono scaduti o la scansione all'accesso non è in esecuzione, Windows invia anche un messaggio di avvertenza per segnalare il problema. Quando il simbolo del Centro sicurezza viene visualizzato, è possibile fare clic su di esso per visualizzare e modificare le impostazioni di Windows.

Se nella barra delle applicazioni viene visualizzata questa icona,

significa che si è verificata una di queste situazioni:

1. La Scansione all'accesso è installata ma è stata disattivata manualmente. Per avviare la Scansione all'accesso, selezionare il collegamento dal menu oppure la scheda Avvio nel percorso **Norman Virus Control|Componenti|Avvio** dell'Editor di Configurazione. Selezionare *Scansione all'accesso* e fare clic su **Salva**.
2. Probabilmente in precedenza è stata selezionata l'opzione **Riavvia più tardi** ed NVC è in attesa che venga riavviato il sistema.
3. Un errore di installazione che potrebbe essere corretto riavviando il sistema.

File di definizione dei virus obsoleti

Un triangolo giallo *lampeggiante* indica che i file di definizione dei virus sono scaduti, ovvero sono vecchi di almeno dieci giorni. Lo stesso si verifica se la scansione all'accesso è disattivata.

Copyright © 1990-2005 Norman

Icone di informazione

Se l'icona Norman viene visualizzata con una rotella, Norman Program Manager sta lavorando con il programma, probabilmente a un'attività di aggiornamento. Si consiglia di non spegnere la macchina quando NPM è in funzione, ovvero quando viene visualizzato questo simbolo.

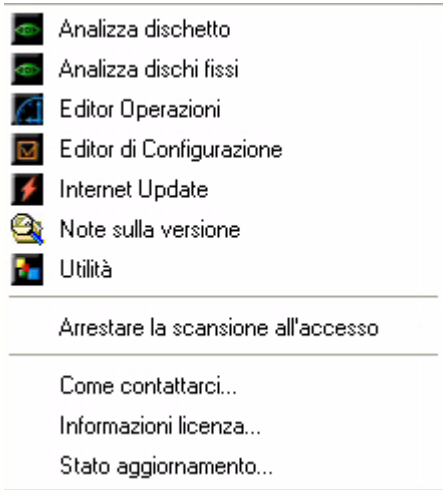
Editor di Configurazione

Norman Virus Control (NVC) ha una serie di componenti che vengono configurati durante l'installazione. Al termine dell'installazione, è possibile rimuovere i componenti non desiderati. NVC è un'applicazione basata su plug-in ed è probabile che con l'evolversi delle nuove tecnologie e in presenza di nuovi attacchi alla sicurezza dei sistemi vengano introdotti nuovi plug-in, ovvero nuovi programmi.

Comune a tutte le schede:

In un ambiente di rete il **campo Accesso** nella parte inferiore di tutte le schede viene visualizzato solo se si hanno i diritti di amministratore. L'amministratore del sistema stabilisce gli elementi da rendere visibili e/o configurabili dalle workstation. L'utente normale può pertanto vedere tutte o alcune delle schede, ma può non essere autorizzato a modificare le impostazioni.

Copyright © 1990-2005 Norman



L'Editor di Configurazione consente una gestione centralizzata della configurazione delle diverse funzioni di NVC. Selezionare *Editor di Configurazione* dal gruppo/cartella Norman visualizzato quando si fa clic con il pulsante destro del mouse sulla 'N' verde nella barra delle applicazioni:

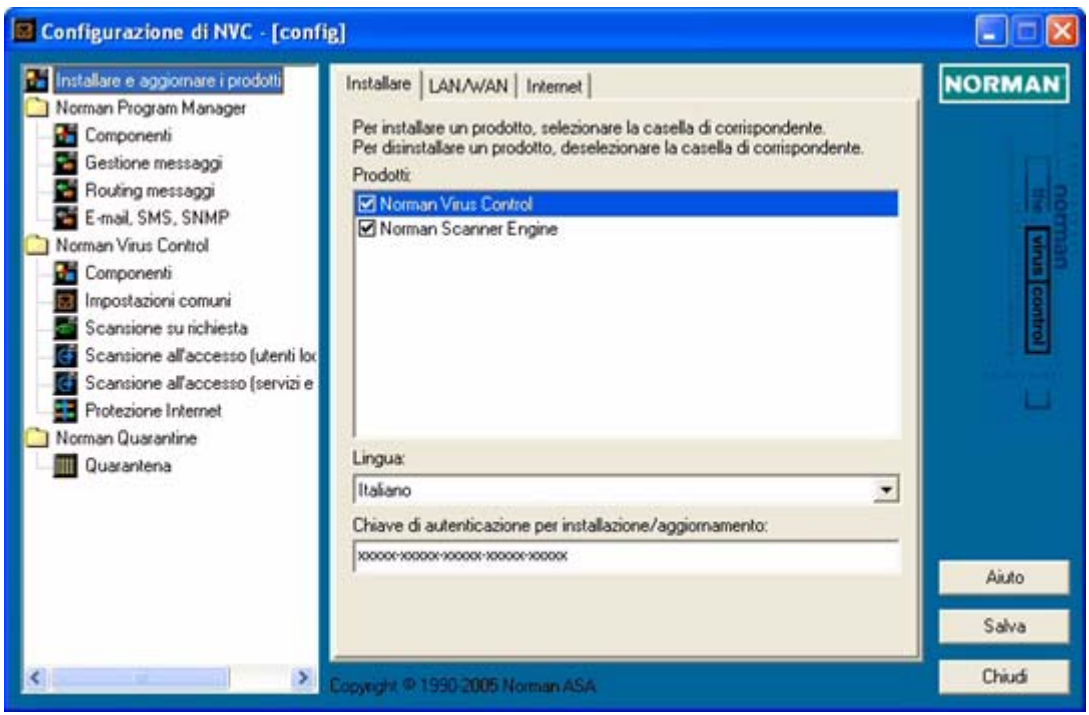
L'elenco comprende i componenti installati. Alcuni componenti, quali ad esempio *Routing messaggi* e *E-mail, SMS, SNMP*, non vengono visualizzati nelle installazioni autonome per utente singolo.

Ogni componente ha una propria finestra di dialogo con schede che contengono una serie di opzioni di configurazioni. Fare clic sul componente che si desidera configurare e selezionare le opzioni desiderate nella scheda corrispondente della finestra di dialogo.

Copyright © 1990-2005 Norman

Installazione e aggiornamento dei prodotti

Installazione



☑ Norman Virus Control

Qualsiasi installazione di NVC richiede l'installazione di questi due prodotti; il prodotto effettivo Norman Virus Control e il prodotto che ne rende possibile l'attività, ossia il motore di scansione (Scanner Engine). Poiché in questa interfaccia utente sono disponibili più prodotti, ad esempio il firewall di Norman o *NVC for Domino*, i prodotti verranno inclusi nell'elenco una volta installati.

Copyright © 1990-2005 Norman

☑ **Norman Scanner Engine**

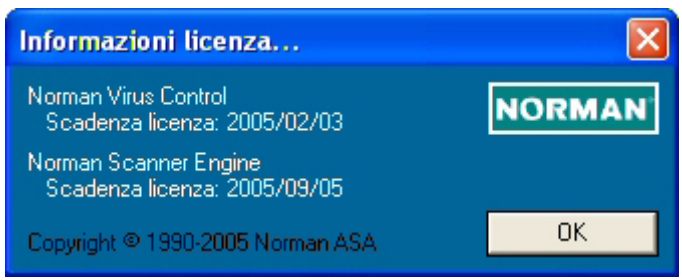
Il motore di scansione rappresenta il fulcro della tecnologia di qualsiasi applicazione antivirus. È possibile considerare l'interfaccia utente come l'involucro, che risulta inutile senza il motore di scansione e i componenti di Norman Program Manager (vedere pagina 32).

Lingua:

Selezionare dal menu a discesa la lingua desiderata per i componenti. Fare clic sulla freccia per visualizzare le lingue disponibili. Questo elenco viene aggiornato man mano che vengono aggiunte versioni in altre lingue.

Chiave di autenticazione per l'installazione o l'aggiornamento:

Si tratta del numero di serie ricevuto all'acquisto di NVC e immesso dall'utente nel corso dell'installazione. Il numero appare in questo campo e contiene informazioni relative alla licenza che consentono di utilizzare NVC in conformità con il Contratto di licenza. Per visualizzare le informazioni sulla licenza, fare clic con il pulsante destro del mouse sull'icona Norman e selezionare *Informazioni licenza* dall'elenco:



Aggiornamento di NVC

Per poter far fronte all'arrivo quotidiano di nuovi virus, Norman provvede ad aggiornare frequentemente i file di definizione dei virus oltre a fornire aggiornamenti regolari del programma.

Nota: I file di definizione dei virus e gli altri componenti sono così integrati che è necessario aggiornare **tutti** i

Copyright © 1990-2005 Norman

componenti disponibili. Non è sufficiente installare solo i file di definizione aggiornati.

È possibile aggiornare NVC in diversi modi: tramite Internet, tramite la rete interna o dal CD del programma. I meccanismi di aggiornamento sono predisposti sia per i server e le reti sia per le macchine indipendenti ed è possibile scegliere tra numerose opzioni di configurazione.

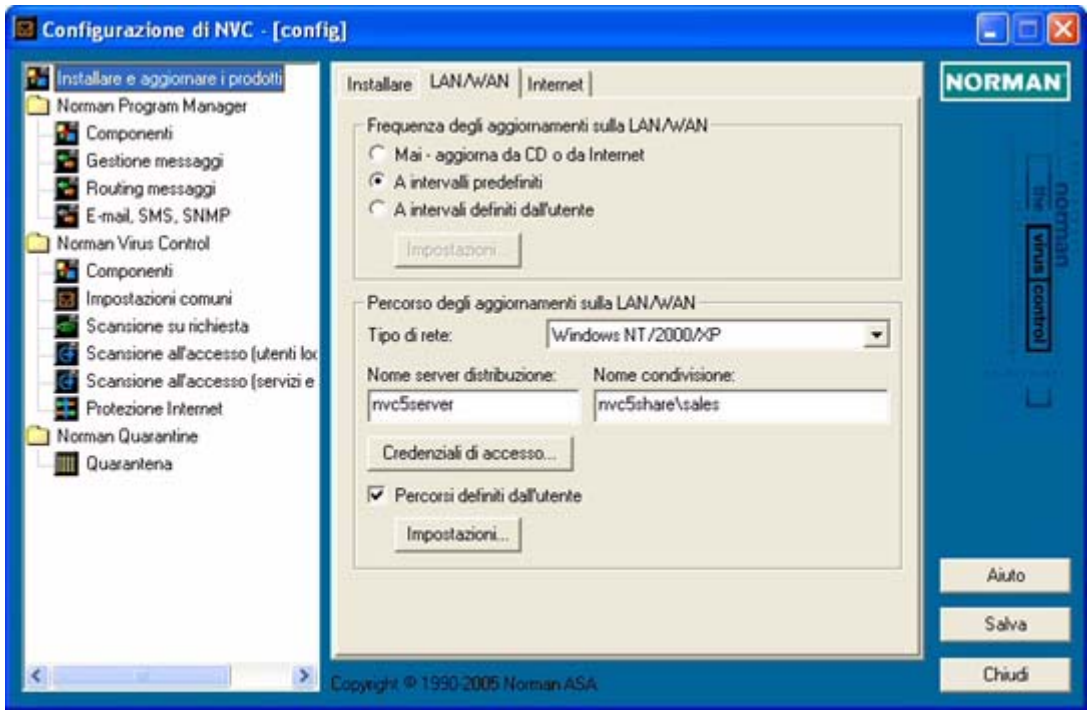
LAN/WAN

Nota: Prima di effettuare modifiche in questa finestra, consultare ***tassativamente*** le istruzioni dettagliate fornite nel *Manuale dell'amministratore*.

Questa scheda consente di aggiornare NVC nelle reti e pertanto è riservata agli amministratori di sistema.

In questa finestra di dialogo è possibile immettere le informazioni richieste sulla rete, impostare la frequenza con cui NVC deve cercare gli aggiornamenti del software, dei file di configurazione e dei file Operazione e configurare le diverse opzioni.

Copyright © 1990-2005 Norman



Frequenza degli aggiornamenti sulla LAN/WAN

- **Mai (aggiorna da CD o da Internet)**

Se non si desidera aggiornare NVC tramite la rete interna, selezionare questa opzione e passare alla finestra di dialogo successiva per specificare come si desidera aggiornare NVC da Internet. Questa opzione si utilizza anche quando si riceve da Norman una versione aggiornata del software su CD-ROM.

Nota: quando si riceve il CD-ROM, i file di definizione dei virus saranno già scaduti e sostituiti da versioni più recenti disponibili sul server Norman. Ciò è dovuto ai tempi di produzione e spedizione intercorsi. Mentre i nuovi file sono subito disponibili su Web, occorrono una o due settimane per preparare e distribuire gli stessi file su CD-ROM. Ogni volta che si installa una nuova versione da CD-ROM, verificare ***sempre*** se sul server di Norman esistono nuovi file di definizione o altri aggiornamenti del software. Norman fornisce uno

Copyright © 1990-2005 Norman

strumento specifico per questo scopo: Norman Internet Update (NIU). Vedere pagina 104.

⊙ A intervalli predefiniti

Gli aggiornamenti vengono eseguiti a intervalli prestabiliti da Norman Program Manager (NPM). NPM opera una distinzione tra i server di distribuzione di NVC e i client.

⇨ Consultare il capitolo su NMP nel *Manuale dell'amministratore*, in particolare la sezione "Intervalli di aggiornamento e traffico di rete", per informazioni dettagliate su questi meccanismi.

○ A intervalli definiti dall'utente

Questa opzione consente di specificare gli intervalli di aggiornamento del software, dei file di configurazione e dei file Operazione. Fare clic su **Impostazioni** per visualizzare la seguente finestra di dialogo:

L'impostazione predefinita per tutti gli aggiornamenti è "A intervalli predefiniti" e sostituisce l'opzione "Automaticamente dal server" disponibile nelle versioni precedenti di NVC5. Se si seleziona l'intervallo predefinito, gli aggiornamenti vengono replicati dal server di distribuzione circa 3 minuti dopo il login e successivamente ogni ora sulle workstation e ogni 5 minuti sui server di distribuzione. Le impostazioni descritte sono quelle predefinite, ma è possibile configurare altri schemi di aggiornamento. Selezionare gli altri intervalli di aggiornamento dai menu a discesa della finestra di dialogo.

Nota: Se non si dispone di una connessione permanente a Internet, si sconsiglia l'opzione predefinita per evitare

Copyright © 1990-2005 Norman

costose connessioni via modem. È preferibile, ad esempio, selezionare un intervallo di un'ora. Inoltre, con una connessione via modem a Internet è necessario che il server di distribuzione sia locale.

Percorso degli aggiornamenti sulla LAN/WAN

Una volta immessi gli intervalli di aggiornamento, è necessario specificare dove si trovano gli aggiornamenti.

Innanzitutto specificare la rete utilizzata selezionandola dall'elenco **Tipo di rete**. È possibile scegliere tra:

- Windows NT/2000/XP/2003
- Workgroup o rete peer-to-peer
- Novell NetWare.

Per Windows NT/2000/XP/2003 e Workgroup o rete peer-to-peer, immettere:

- Nome server distribuzione
- Condivisione

Per Novell NetWare immettere:

- Nome server distribuzione
- Nome volume e directory principale

Nota: immettere il nome del server di distribuzione senza barre rovesciate o altri caratteri speciali.

Una volta inseriti i valori nei tre campi di *Percorso degli aggiornamenti sulla LAN/WAN* , NVC interpreta le informazioni per stabilire quali sono i percorsi completi dei file.

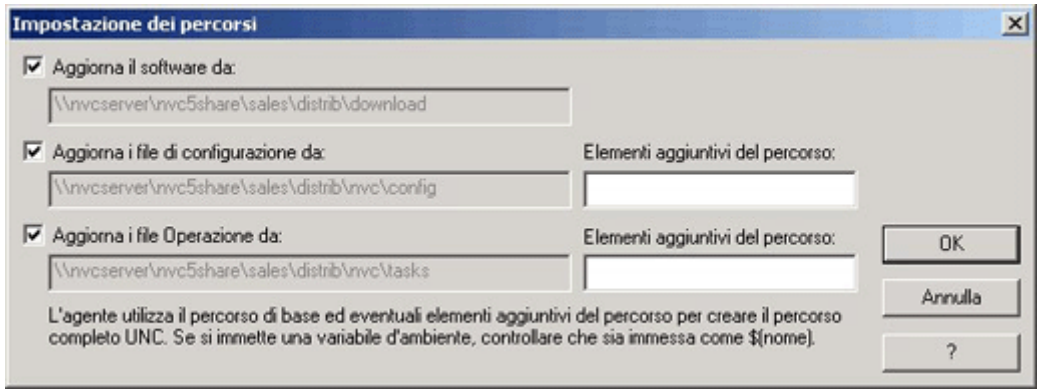
Credenziali di accesso

Se si utilizza una rete Windows, è possibile immettere il nome utente, la password e il nome del dominio facendo clic sul pulsante **Credenziali di accesso**.

Percorsi definiti dall'utente

Se, ad esempio, si desidera avere file di configurazione e file Operazione diversi a seconda dei reparti di un'azienda, è necessario selezionare **Percorsi definiti dall'utente** e fare clic su **Impostazioni**. Viene visualizzata la finestra di dialogo seguente:

Copyright © 1990-2005 Norman


Impostazione dei percorsi
Aggiorna il software da:
\\nvcserver\nvc5share\sales\distrib\download
Aggiorna i file di configurazione da:
Elementi aggiuntivi del percorso:
\\nvcserver\nvc5share\sales\distrib\nvc\config
Aggiorna i file Operazione da:
Elementi aggiuntivi del percorso:
\\nvcserver\nvc5share\sales\distrib\nvc\tasks
OK
Annulla
?
L'agente utilizza il percorso di base ed eventuali elementi aggiuntivi del percorso per creare il percorso completo UNC. Se si immette una variabile d'ambiente, controllare che sia immessa come $(nome).

In questa finestra di dialogo i campi contengono già i valori in base alle informazioni specificate in *Nome del server* e *Condivisione* (*Nome volume e directory principale* in Novell).

☑ **Aggiorna il software da:**

Identifica, ad esempio, il percorso del server da cui è possibile prelevare gli aggiornamenti del software NVC dopo averli scaricati da Internet. In questa casella sono visualizzati il nome del server e della condivisione/volume immessi nella finestra di dialogo precedente, oltre al percorso predefinito che indica la posizione in cui si trovano i pacchetti software.

☑ **Aggiorna i file di configurazione da:**

In questa casella sono visualizzati il nome del server e della condivisione/volume immessi nella finestra di dialogo precedente, oltre al percorso predefinito che indica la posizione in cui sono memorizzati i file di configurazione.

☑ **Aggiorna i file Operazione da:**

In questa casella sono visualizzati il nome del server e della condivisione/volume immessi nella finestra di dialogo precedente, oltre al percorso predefinito che indica la posizione in cui sono memorizzati i file Operazione.

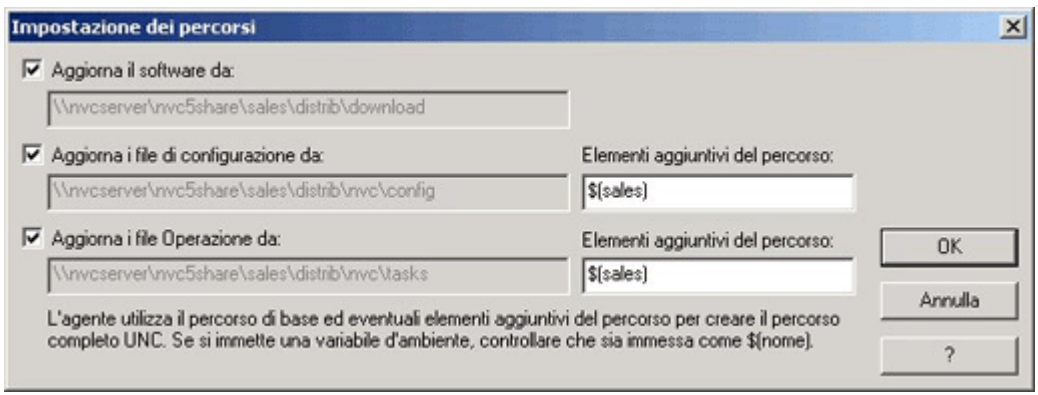
Elementi aggiuntivi del percorso:

Questo ulteriore campo per l'aggiornamento dei *file di configurazione* e dei *file Operazione* consente di distribuire i file

Copyright © 1990-2005 Norman

di configurazione e i file Operazione personalizzati nei diversi reparti di un'azienda.

Se si immette un ulteriore elemento del percorso, controllare che venga specificata anche la variabile di ambiente nel formato $(nome), che consente a NPM di stabilire un percorso UNC completo. Esempio:


Impostazione dei percorsi
Aggiorna il software da:
\\nvcserver\nvc5share\sales\distrib\download
Aggiorna i file di configurazione da:
\\nvcserver\nvc5share\sales\distrib\nvc\config
Elementi aggiuntivi del percorso:
$(sales)
Aggiorna i file Operazione da:
\\nvcserver\nvc5share\sales\distrib\nvc\tasks
Elementi aggiuntivi del percorso:
$(sales)
L'agente utilizza il percorso di base ed eventuali elementi aggiuntivi del percorso per creare il percorso completo UNC. Se si immette una variabile d'ambiente, controllare che sia immessa come $(nome).
OK
Annulla
?

Internet

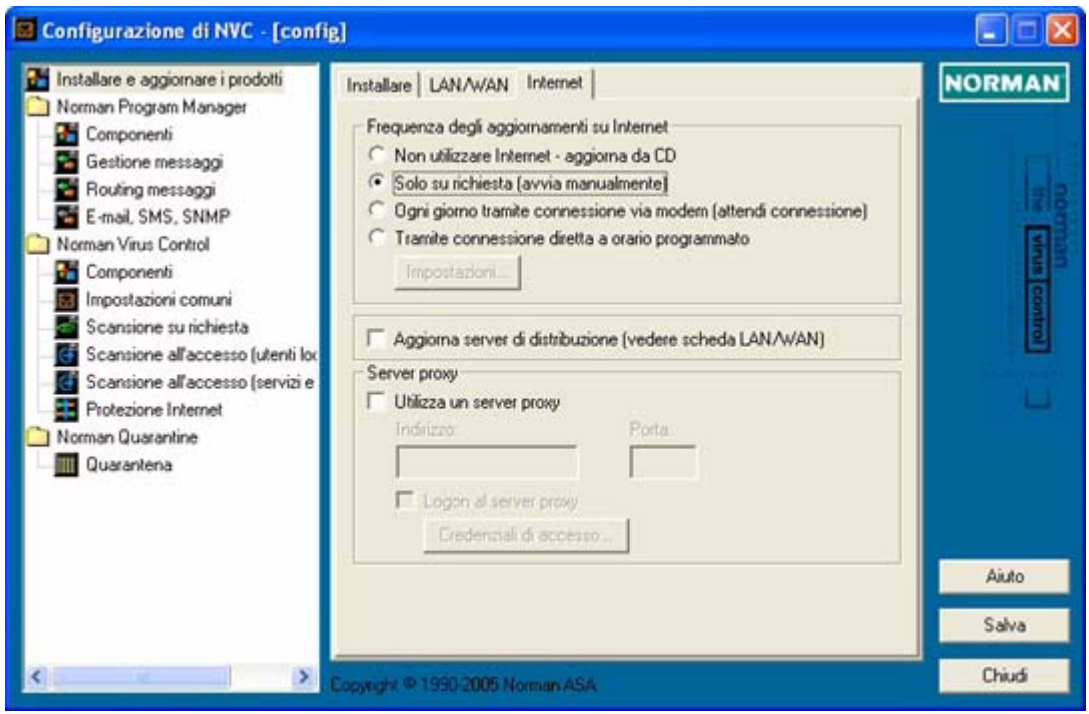
Le selezioni effettuate in questa sezione determinano la gestione degli aggiornamenti da Internet da parte di Internet Update (IU).

Internet è il metodo più pratico e veloce per distribuire i file di definizione dei virus aggiornati e gli aggiornamenti degli altri componenti di NVC. Per mantenere la protezione totale è necessario scaricare tutti questi aggiornamenti non appena disponibili. Quindi è importante scegliere con attenzione l'opzione che meglio si adatta alle proprie esigenze.

Il programma Internet Update (IU) gestisce gli aggiornamenti di NVC. Tali aggiornamenti sono disponibili sotto forma di pacchetti e IU è in grado di stabilire quali pacchetti sono idonei per la piattaforma e la lingua dell'utente. Tuttavia su una rete spesso vengono eseguiti più sistemi operativi e versioni in lingue diverse di NVC. In ambienti eterogenei è necessario, pertanto, eseguire uno strumento di configurazione separato di IU (NIUcf), per essere certi che vengano scaricati gli aggiornamenti

Copyright © 1990-2005 Norman

per tutta la rete. NIUcf è descritto nelle sezioni "Installazione e distribuzione" per Windows NT e Novell NetWare del *Manuale dell'amministratore.*



Frequenza degli aggiornamenti su Internet

Nota: Se il computer è protetto da un firewall o da un server proxy, potrebbe essere necessario immettere le informazioni richieste nella sezione **Server proxy** di questa finestra di dialogo (pagina 29).

- **Non utilizzare Internet – aggiorna da CD**

Se si seleziona questa opzione, non verranno mai visualizzati messaggi o promemoria relativi ai download disponibili da Internet. Dato che di solito i CD vengono distribuiti solo quando viene rilasciata una nuova versione di NVC, si riceveranno solo CD da Norman circa ogni tre mesi. **Non** si consiglia questa opzione perché nel giro di una settimana l'installazione di NVC non sarà più aggiornata.

Copyright © 1990-2005 Norman

⊙ **Solo su richiesta (avvia manualmente)**

Selezionare questa opzione se si preferisce avviare IU manualmente dal menu di NVC per controllare se sono disponibili degli aggiornamenti oppure utilizzare l'utilità **Operazioni pianificate** di Windows (che si trova nel **Pannello di controllo)**.

O **Ogni giorno tramite connessione via modem (attendi connessione)**

Se si utilizza un modem per collegarsi a Internet, selezionare questa opzione per poter verificare ogni giorno la presenza di eventuali aggiornamenti sui server di Norman. L'accesso a Internet avviene normalmente, quindi il programma rileva la disponibilità o meno di file aggiornati.

Se la connessione a Internet avviene diverse volte al giorno, IU ricercherà gli aggiornamenti solo nel corso della prima connessione. Se, ad esempio, la connessione a Internet avviene una volta alla settimana, IU eseguirà la ricerca la prima volta, alla connessione.

O **Tramite connessione diretta a orario programmato**

È possibile selezionare questa opzione se si è provvisti di una connessione permanente a Internet. Fare clic su **Specify** per pianificare un orario:

Per prima cosa occorre specificare l'orario in cui NVC deve effettuare la ricerca di aggiornamenti. Immettere l'orario, quindi utilizzare il menu a discesa '+-' per fornire al sistema un intervallo di tempo opportuno in cui inserire le operazioni pianificate evitando possibili sovraccarichi.

Copyright © 1990-2005 Norman

Nota: se Internet Update non è stato eseguito per 24 ore, il programma verifica automaticamente gli aggiornamenti all'avvio.

☐ **Aggiorna server di distribuzione (vedere scheda LAN/WAN)**

Se si seleziona questa opzione, si consente a un client di scaricare gli aggiornamenti da un server di distribuzione di NVC. Per poter effettuare l'aggiornamento, è necessario che l'utente connesso abbia accesso in scrittura alla directory di distribuzione (…`\Norman\Distrib\Download`).

L'opzione **Aggiorna server di distribuzione** non è un'opzione predefinita. Pertanto, i client che tentano di eseguire Internet Update (NIU.EXE) aggiornano il percorso di download (`...\Norman\Download`) e non la directory di distribuzione (`...\Norman\Distrib\Download`). Questa opzione risulta utile, ad esempio, per i laptop: quando l'utente è in ufficio, il laptop viene aggiornato dal server di distribuzione, mentre quando è in viaggio viene aggiornato eseguendo Internet Update.

Se sul *client* in cui è in esecuzione IU è abilitata l'opzione **Aggiorna server di distribuzione** e il client non è connesso alla rete, non vengono aggiornati né l'installazione locale di NVC né il server di distribuzione.

Se si esegue IU dal *server di distribuzione*, si consiglia di non selezionare **Aggiorna server di distribuzione**.

In genere, l'opzione **Aggiorna server di distribuzione** viene selezionata solo per un paio di computer che di solito sono sempre connessi alla rete. Per ulteriori informazioni, consultare la sezione sulla distribuzione di file di configurazione e Operazione diversi sulle singole workstation nel *Manuale dell'amministratore*.

Nelle installazioni in cui Novell Netware è il server di distribuzione, questa opzione deve essere selezionata per almeno una macchina (ad esempio la macchina dell'amministratore di NVC).

Server proxy

I server proxy possono richiedere l'autenticazione dell'utente. Se si utilizzano le opzioni per server proxy di questa finestra di

Copyright © 1990-2005 Norman

dialogo, è necessario immettere qui le stesse informazioni di logon al server proxy e di autenticazione configurate sul proxy.

I due schemi di autenticazione principali sono:

1. Base e
2. Windows NT challenge/response, detto anche NTLM.

Server proxy

☐ **Usa un server proxy**

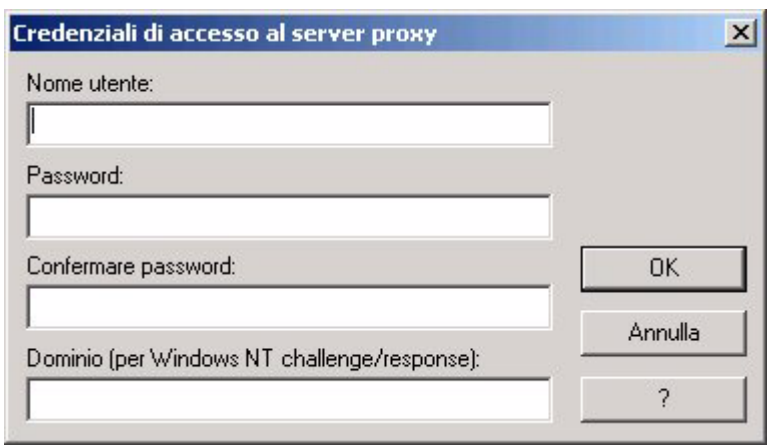
Immettere l'**Indirizzo** e la **Porta** del proxy HTTP del firewall.

Se le informazioni per il proxy HTTP sono state specificate nel browser, sarà necessario immettere esattamente le stesse impostazioni.

☐ **Logon al server proxy**

Nota: Questa opzione è pertinente solo nel caso in cui il server proxy richieda l'autenticazione.

Fare clic su **Credenziali di accesso** per visualizzare questa finestra di dialogo:



È necessario che le informazioni immesse in questa finestra di dialogo corrispondano a quelle normalmente specificate per effettuare il logon al server proxy.

Nome utente:

Immettere un nome utente valido.

Copyright © 1990-2005 Norman

Password:

Immettere la password.

Dominio (per Windows NT challenge/response)

Questo campo non è applicabile per i server proxy che utilizzano l'autenticazione di base.

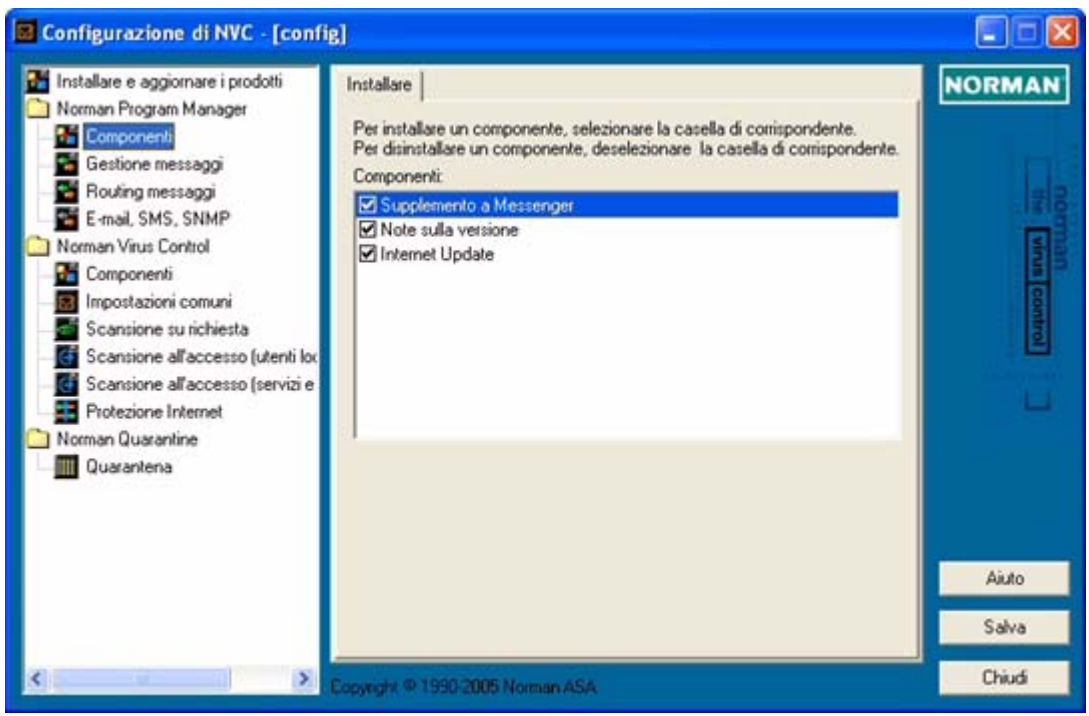
Immettere il nome del dominio. Nel caso in cui il campo venga lasciato vuoto, verrà utilizzato il *nome della macchina*.

Copyright © 1990-2005 Norman

Norman Program Manager

Questa cartella è costituita dai tre moduli proprietari Norman che gestiscono la comunicazione interna tra i diversi componenti del prodotto.

Il routing dei messaggi consente agli amministratori di selezionare che tipo di messaggi verranno inviati agli altri PC in rete su cui viene eseguito NVC. Per una descrizione tecnica dettagliata del sistema di messaggistica, consultare il capitolo "Messaggi" nel *Manuale dell'amministratore*.



Copyright © 1990-2005 Norman

Componenti

Installazione

☑ **Supplemento a Messenger**

In base alla licenza di cui si dispone, il Supplemento a Messenger fornisce ulteriori moduli di messaggistica, ossia la funzionalità per SMS, SNMP ed e-mail, particolarmente utile in un ambiente di rete. Questo modulo viene descritto dettagliatamente a pagina 42.

☑ **Note sulla versione**

Fornisce informazioni utili sulla versione corrente e su quelle successive in un formato leggibile con un browser Web. Contiene anche collegamenti ad aree di download, ecc.

☑ **Internet Update**

Utilizzare questo strumento per scaricare automaticamente l'ultima versione di NVC. Internet Update può essere configurato per scaricare gli aggiornamenti a intervalli pianificati.

⇨ ‘Norman Internet Update' a pagina 104.

Informazioni su messaggistica e log

Il sistema di messaggistica consente di stabilire quali eventi si desidera che vengano segnalati.

Il modo tradizionale con cui viene generato un log è scrivere dei messaggi in un file di log. In NVC v5 questa funzione viene gestita da uno dei moduli di output standard caricati da NPM. Pertanto, i messaggi ricevuti da NPM vengono passati al modulo di output del file di log **Messaggi** del gruppo **Utilità** (pagina 101).

Gestione messaggi

Gestione messaggi seleziona i messaggi per il file di log, visualizza i messaggi sulla console messaggi e determina il contenuto del Log degli eventi di Windows NT/2000/XP/2003. Infine, è disponibile un'opzione per definire i messaggi da

Copyright © 1990-2005 Norman

trasmettere. In questo modo vengono aggiunte quattro finestre di dialogo con schede in questa finestra, con opzioni identiche nelle prime tre finestre. Le selezioni effettuate determinano i messaggi che appariranno nel file di log di NVC, nella console messaggi e nel Log degli eventi di Windows NT/2000/XP/2003.

Su OS/2 NVC memorizza i messaggi nel *log degli errori di sistema*.

La gestione dei messaggi consente agli utenti nonché agli amministratori di selezionare quali messaggi visualizzare e quali conservare *localmente*. Questa funzione consente di tenere sotto controllo tutte le attività dei componenti di NVC localmente e nella rete.

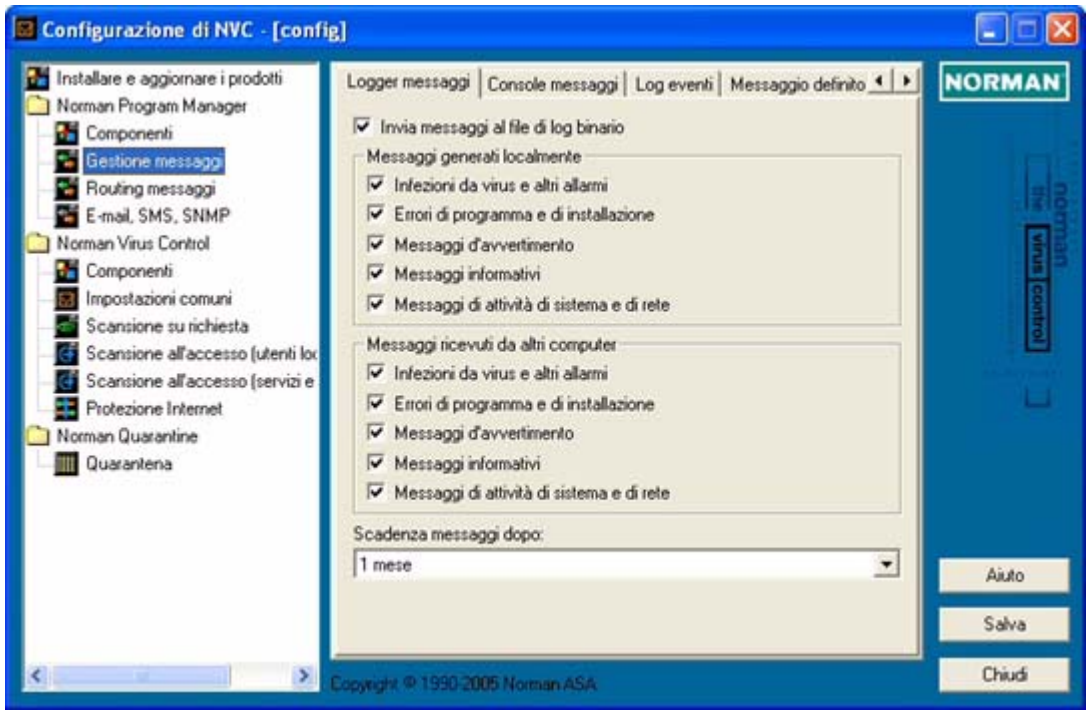
Quando il **Logger messaggi** è attivato, i messaggi generati localmente e/o i messaggi ricevuti da altre macchine vengono *inviati* al file di log binario.

Quando la **Console messaggi** è attivata, i messaggi generati localmente e/o i messaggi ricevuti da altre macchine vengono *inviati* alla console dei messaggi.

Quando il **Log degli eventi** è attivato, i messaggi generati localmente e/o i messaggi ricevuti da altre macchine vengono *inviati* al Log degli eventi di Windows NT/2000/XP/2003.

Copyright © 1990-2005 Norman

Logger messaggi



☑ Invia messaggi al file di log binario

Per accedere alle altre opzioni presenti in questa finestra di dialogo, selezionare questa opzione. In caso contrario il Logger dei messaggi resterà disattivato.

Nota: Il file di log binario è crittografato e può essere visualizzato solo dal modulo **Utilità** (componente **Messaggi**). Consultare la pagina 101. Vengono creati anche file di log di testo, con gli stessi criteri del file di log binario. Tutti i file di log (di testo e binari) vengono memorizzati nella directory MSG nella directory in cui è installato NVC, solitamente `c:\norman\msg`.

Messaggi generati localmente

In questa sezione è possibile stabilire quali eventi provenienti dalla macchina ***locale*** dovranno apparire nel file di log.

Copyright © 1990-2005 Norman

☑ **Infezione da virus e altri allarmi**

Crea voci nel file di log relative al rilevamento di virus o altro codice dannoso.

☑ **Errori di programma e di installazione**

Crea voci nel file di log relative a errori segnalati da un programma di NVC installato o verificatisi durante l'installazione di NVC.

☑ **Messaggi di avvertimento**

Crea voci nel file di log relative a messaggi di avvertimento visualizzati.

☐ **Messaggi informativi**

Crea un messaggio di natura informativa. Valutare attentamente questa opzione prima di selezionarla, in quanto vengono generati *molti* messaggi informativi generici.

☑ **Messaggi di attività di sistema e di rete**

Crea voci nel file di log relative ad attività di rete sul sistema. Questa opzione è sempre attiva.

Messaggi ricevuti da altri computer

Nella sezione precedente sono stati selezionati gli eventi verificatisi sulla macchina ***locale*** da inserire nel file di log. In questa sezione è possibile scegliere quali eventi provenienti da ***altri*** computer inserire nel file di log.

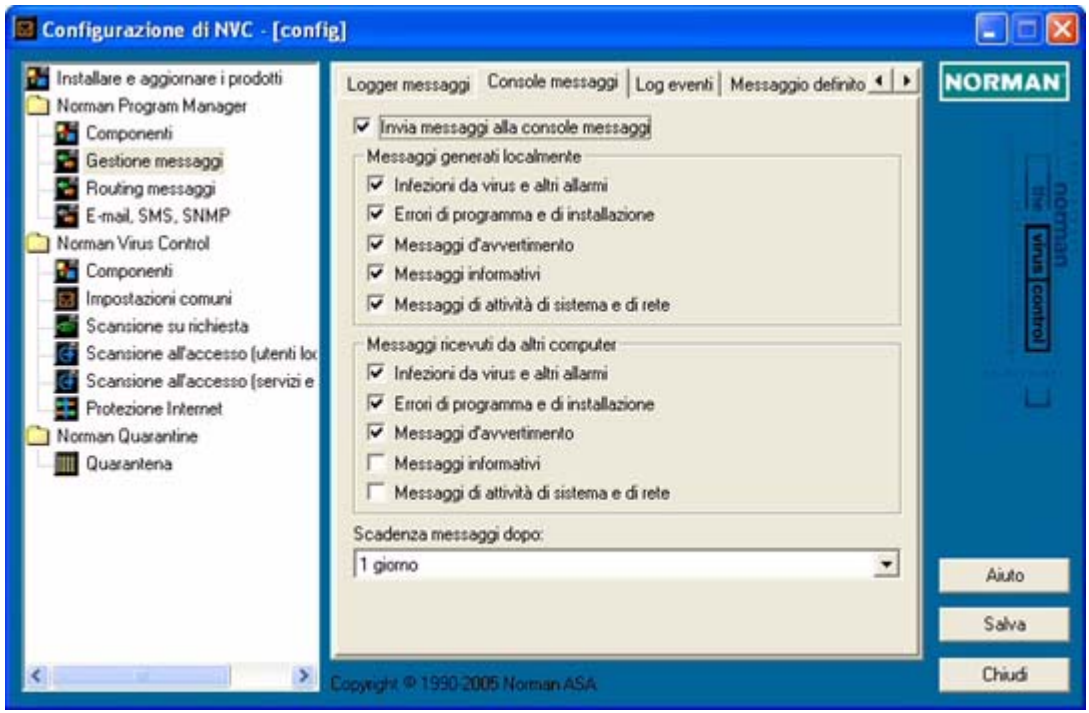
Le opzioni da selezionare sono esattamente le stesse della sezione precedente.

Scadenza messaggi dopo:

Scegliere la durata della permanenza dei messaggi nel file di log tra le possibili opzioni: un giorno, due giorni, una settimana, un mese, mai.

Copyright © 1990-2005 Norman

Console messaggi



È necessario selezionare

☑ **Invia messaggi alla console messaggi**

per accedere alle opzioni di configurazione, che sono identiche a quelle illustrate nella sezione "Logger messaggi" a partire da pagina pagina 35.

Scadenza messaggi dopo:

Scegliere per quanto tempo tenere i messaggi sulla console tra le possibili opzioni: un'ora, otto ore, un giorno, due giorni, una settimana, un mese, mai.

Le opzioni di configurazione rimanenti sono identiche a quelle presenti nella scheda precedente.

Copyright © 1990-2005 Norman

Registro eventi

È necessario selezionare

☑ **Invia messaggi al Log degli eventi di Windows NT/2000**

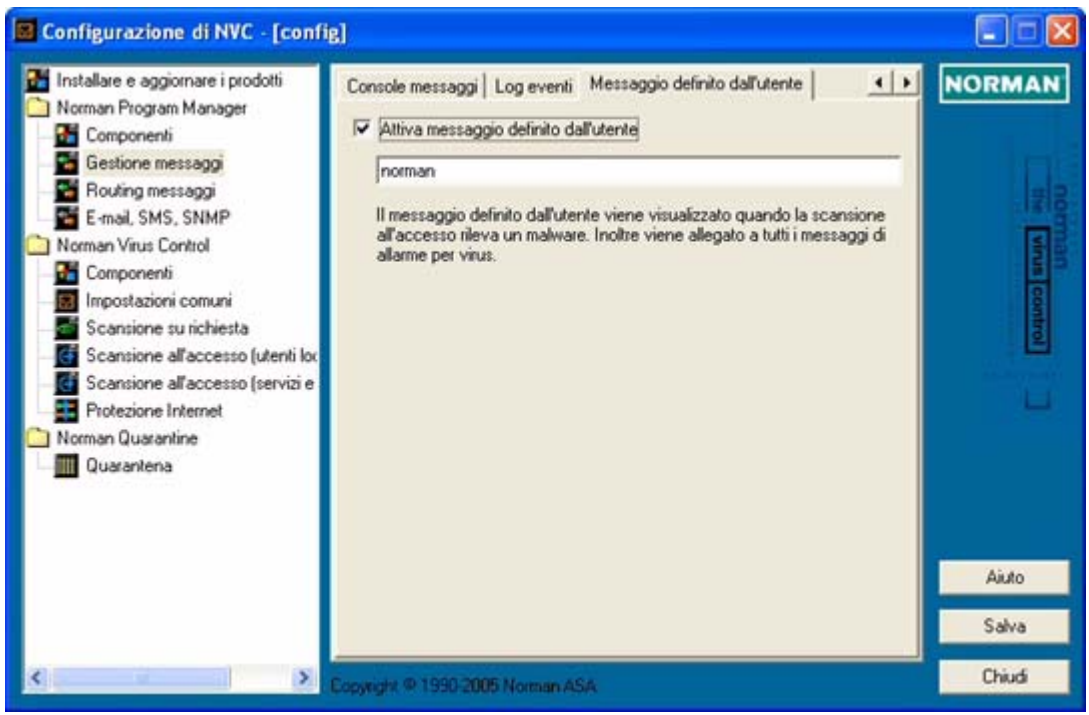
per accedere alle opzioni di configurazione, che sono identiche a quelle illustrate nella sezione "Logger messaggi" a partire da pagina pagina 35.

Messaggio definito dall'utente

È necessario selezionare

☑ **Attiva messaggio definito dall'utente**

per accedere al campo in cui inserire il messaggio.



Quando la Scansione all'accesso rileva un'infezione, sulle workstation viene visualizzato il messaggio immesso in questo campo. Questo messaggio contiene le istruzioni esatte o il

Copyright © 1990-2005 Norman

riferimento alla strategia adottata dall'azienda quando il codice dannoso è diffuso nella rete.

Viene allegato anche ai messaggi trasmessi tramite il sistema interno di trasmissione di NVC.

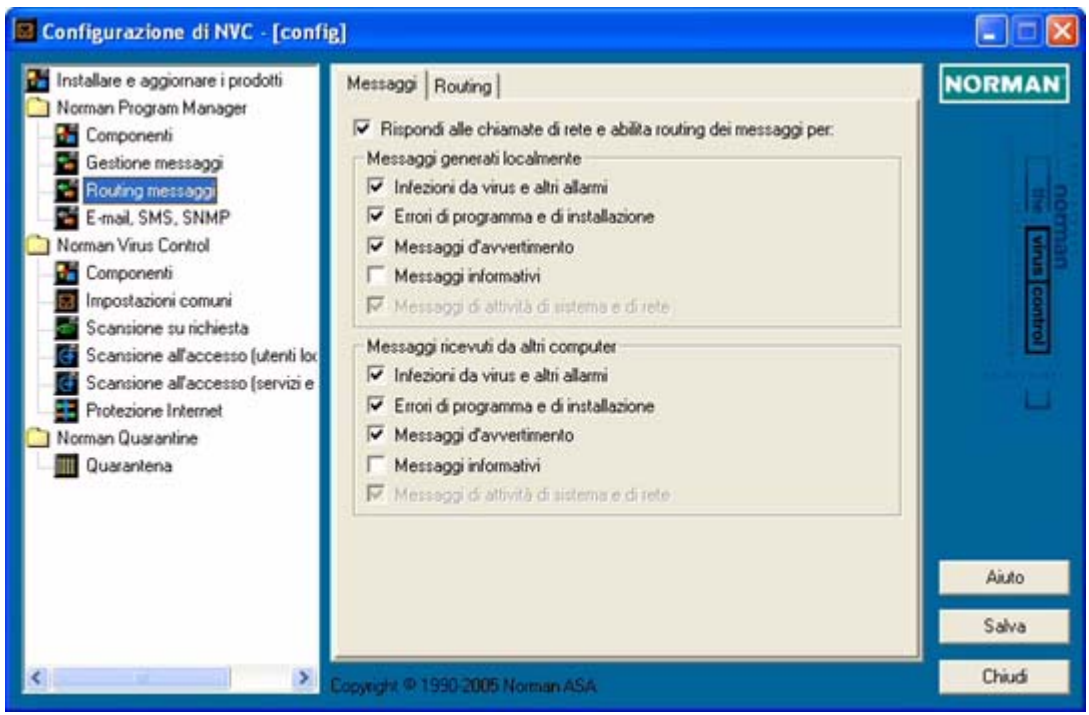
Controllare che nel modulo **Routing messaggi** (pagina 40) siano abilitate le opzioni di trasmissione e di routing. Consultare anche il *Manuale dell'amministratore* per ulteriori informazioni sulla gestione di messaggi e allarmi da parte di NVC.

Copyright © 1990-2005 Norman

Routing messaggi

Nota: Questo modulo è disponibile solo in un'installazione di rete.

Messaggi



Questo modulo di output per messaggi supporta sia le reti IP che IPX e si basa sulla connessione utilizzando il protocollo TCP/IP e/o SPX.

Nota: Per informazioni dettagliate sulla gestione di messaggi e allarmi da parte di NVC consultare il *Manuale dell'amministratore*.

☑ Rispondi alle chiamate di rete e abilita routing dei messaggi per:

Per accedere alle altre opzioni presenti in questa finestra di dialogo, selezionare questa opzione. In caso contrario il router dei messaggi resterà disattivato.

Copyright © 1990-2005 Norman

Per chiamate di rete si intende uno stesso messaggio inviato contemporaneamente a più destinatari.

Messaggi generati localmente

Seleziona quali eventi provenienti dalla macchina ***locale*** devono essere inoltrati dal router dei messaggi.

☑ **Infezione da virus e altri allarmi**

Inoltra un messaggio se rileva un virus o altro codice dannoso.

☑ **Errori di programma e di installazione**

Inoltra un messaggio d'errore rilevato da un programma NVC già installato, o eventuali messaggi d'errore verificatisi durante l'installazione di NVC.

☑ **Messaggi di avvertimento**

Inoltra i messaggi di avvertimento visualizzati.

☐ **Messaggi informativi**

Inoltra un messaggio di natura informativa. Valutare attentamente questa opzione prima di selezionarla, in quanto vengono generati *molti* messaggi informativi generici.

☑ **Messaggi di attività di sistema e di rete**

Invia messaggi relativi alle attività di rete sul sistema. Questa opzione è sempre attiva.

Messaggi ricevuti da altri computer

La sezione precedente consentiva di selezionare gli eventi provenienti dalla macchina ***locale*** da inoltrare. In questa sezione è possibile scegliere quali messaggi relativi ad eventi provenienti da ***altri*** computer inoltrare.

Le opzioni da selezionare sono esattamente le stesse della sezione precedente.

Routing

Se il routing dei messaggi è attivo, specificare i destinatari in questa sezione.

Inoltra messaggi in arrivo a:

Copyright © 1990-2005 Norman

Fare clic su **Aggiungi** e immettere l'indirizzo IP o il nome del computer del destinatario. L'operazione va ripetuta per ogni destinatario che si desidera aggiungere all'elenco. Nomi e indirizzi possono essere modificati o rimossi dall'elenco facendo clic sui pulsanti appropriati.

Di norma si deve specificare un solo destinatario per evitare la duplicazione dei messaggi. Per maggiori informazioni, consultare il *Manuale dell'amministratore*.

☑ **Inoltra messaggi**

Selezionare questa opzione per inviare i messaggi in arrivo a uno o più membri dell'elenco. È anche possibile determinare la scadenza dei messaggi in arrivo, scegliendo tra 1, 8 o 24 ore, 1 o 4 settimane o mai. Il valore di default è 1 settimana.

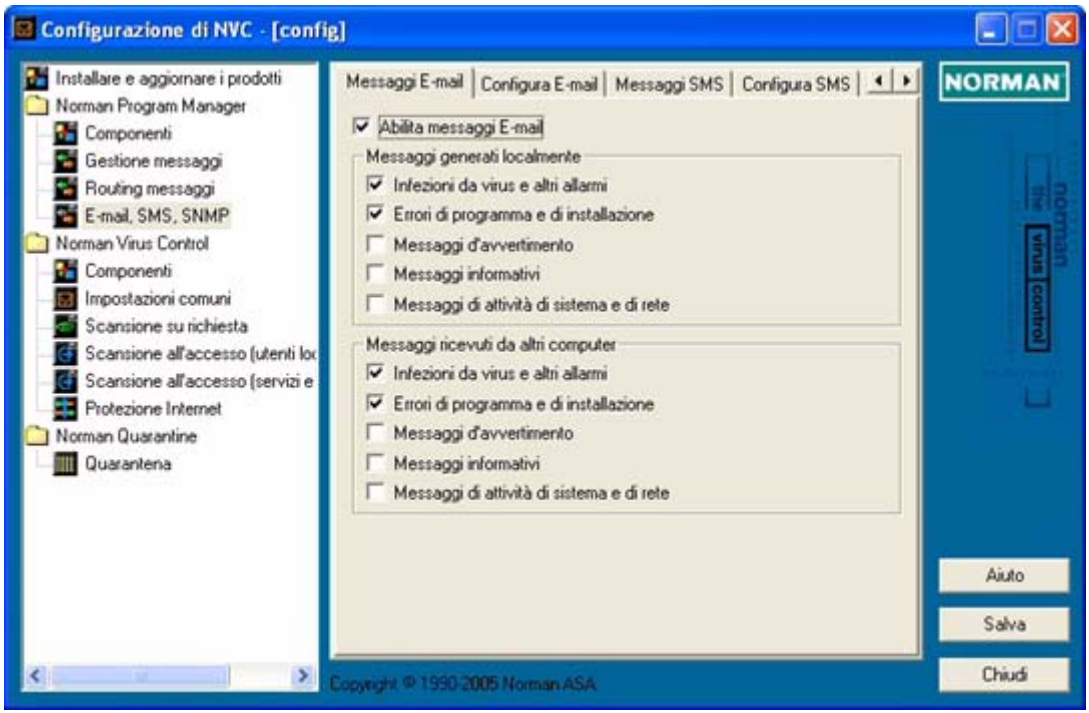
E-mail, SMS, SNMP

Questo modulo consente di inviare messaggi di posta elettronica o messaggi SMS relativi ad eventi selezionati su PC o su computer collegati in rete. Per le reti con SNMP è possibile configurare NVC in modo tale che invii delle trap SNMP.

Messaggi per E-mail, SMS e SNMP

È possibile filtrare gli eventi che producono l'invio di una e-mail, di un messaggio, o di una trap SNMP nello stesso modo in cui si selezionano gli eventi significativi per il **Routing messaggi** e la **Gestione messaggi**, utilizzando le stesse opzioni.

Copyright © 1990-2005 Norman



Per quanto riguarda gli altri moduli per i messaggi, occorre distinguere tra messaggi generati **localmente** e messaggi **ricevuti** da altre macchine.

Impostazioni di default

Le impostazioni di default per i messaggi generati localmente e i messaggi ricevuti da altre macchine sono:

☑ **Infezione da virus e altri allarmi**

Inoltra un messaggio di rilevamento virus o altro codice dannoso.

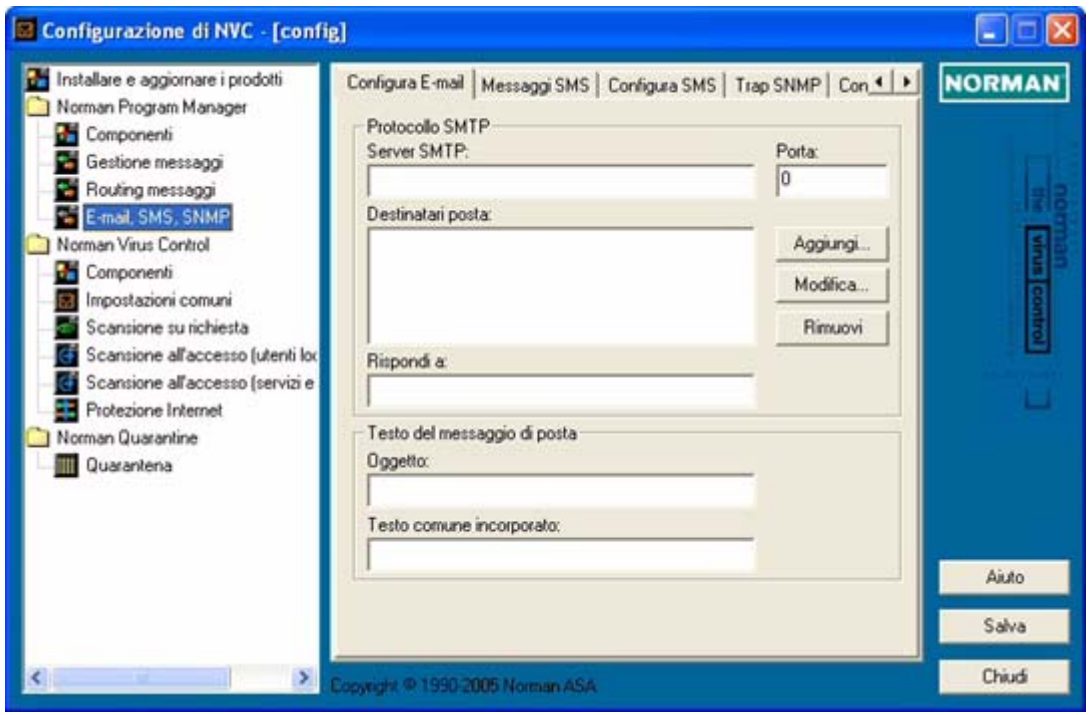
☑ **Errori di programma e di installazione**

Inoltra il messaggio d'errore rilevato da un programma NVC già installato, o eventuali messaggi d'errore verificatisi durante l'installazione di NVC.

Copyright © 1990-2005 Norman

Per i messaggi SMS l'impostazione di default è solo la prima opzione.

Configura messaggi e-mail



Nella sezione Protocollo *SMTP* della finestra di dialogo devono essere compilati i seguenti campi:

Server SMTP

Il nome del server o l'indirizzo IP del server di posta che può ricevere i messaggi SMTP.

Porta

La porta SMTP predefinita è la '25'. Tale valore è da ritenersi corretto a meno che non si sia esplicitamente selezionata un'altra porta.

Destinatari posta

Immettere gli indirizzi e-mail dei destinatari del messaggio.

Copyright © 1990-2005 Norman

- Premere il pulsante **Aggiungi** per inserire l'indirizzo e-mail di un destinatario del messaggio.
- Selezionare un indirizzo dall'elenco e fare clic su **Modifica** per modificare un indirizzo esistente.
- Selezionare un indirizzo dall'elenco e fare clic su **Rimuovi** per eliminare un indirizzo esistente.

Rispondi a

Immettere l'indirizzo e-mail a cui il destinatario può rispondere, per esempio quello dell'amministratore del sistema.

Nella sezione *Testo del messaggio di posta* è possibile specificare:

Oggetto

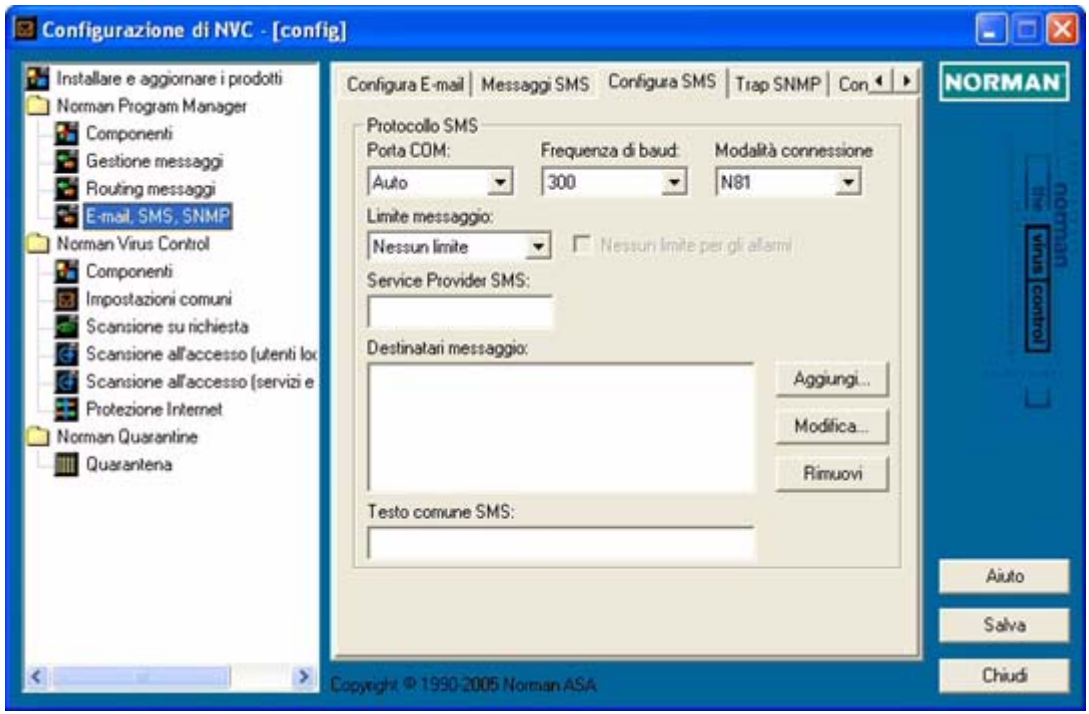
Il titolo del messaggio di posta, ad esempio, "Messaggio di NVC". Potrebbe essere una buona idea riportare l'evento che ha causato il messaggio di posta, se era stata scelta solo un'alternativa, ad esempio **Infezioni da virus e altri allarmi**.

Testo comune incorporato

Inserire il testo che si desidera includere nel messaggio di posta come nota a piè di pagina predefinita.

Copyright © 1990-2005 Norman

Configura messaggi SMS



Compilare i seguenti campi:

Porta COM

Specificare la porta COM SMS scegliendo dall'elenco nel menu a discesa. Questa è la porta specificata quando si imposta come modem il cellulare utilizzando il driver fornito dal produttore. Se non si conosce il numero della porta, selezionare "Auto" e lasciare che il programma identifichi la porta corretta.

Frequenza di baud

La frequenza di baud specifica i parametri di comunicazione seriale che vengono applicati al modem GSM. Se non si conosce la frequenza di baud, fare riferimento alla documentazione tecnica del modem. NVC supporta il set di comandi Extended Hayes per SMS – "ETSI GSM 07.07" e una serie di test ha

Copyright © 1990-2005 Norman

evidenziato che il modem più indicato è il Falcom GSM Modem (per dettagli, vedere: ***www.falcom.de***.)

Modalità connessione

Il formato più comune per le comunicazioni seriali è **N81**. Fare clic sul menu a discesa per visualizzare ulteriori opzioni.

Limite messaggio

È possibile limitare il numero di messaggi che si possono inviare in un determinato intervallo di tempo. Se non si desidera accettare il valore di default "Nessun limite", scegliere un altro valore dal menu a discesa.

1/15 denota un messaggio ogni 15 minuti

1/ora denota un messaggio ogni ora, ecc.

Notare che se, ad esempio, si seleziona l'opzione 1/15,*tutti* i messaggi successivi al primo nell'intervallo di 15 minuti verranno persi.

☑ **Nessun limite per gli allarmi**

Questa opzione è ***attiva*** per default, se si seleziona un qualsiasi limite, ad eccezione di 'Nessun limite'. Questo serve a garantire che non venga perso alcun messaggio importante (gli allarmi), a causa del fatto che messaggi meno importanti hanno esaurito il limite specificato per i messaggi. Se si specifica solo "Infezioni da virus e altri allarmi" e l'opzione sopraindicata è attiva, agli allarmi non verrà applicato nessun limite.

Service Provider SMS

Immettere il numero di telefono del service provider SMS.

Destinatari messaggio

Inserire il numero telefonico di tutti i destinatari dei messaggi SMS.

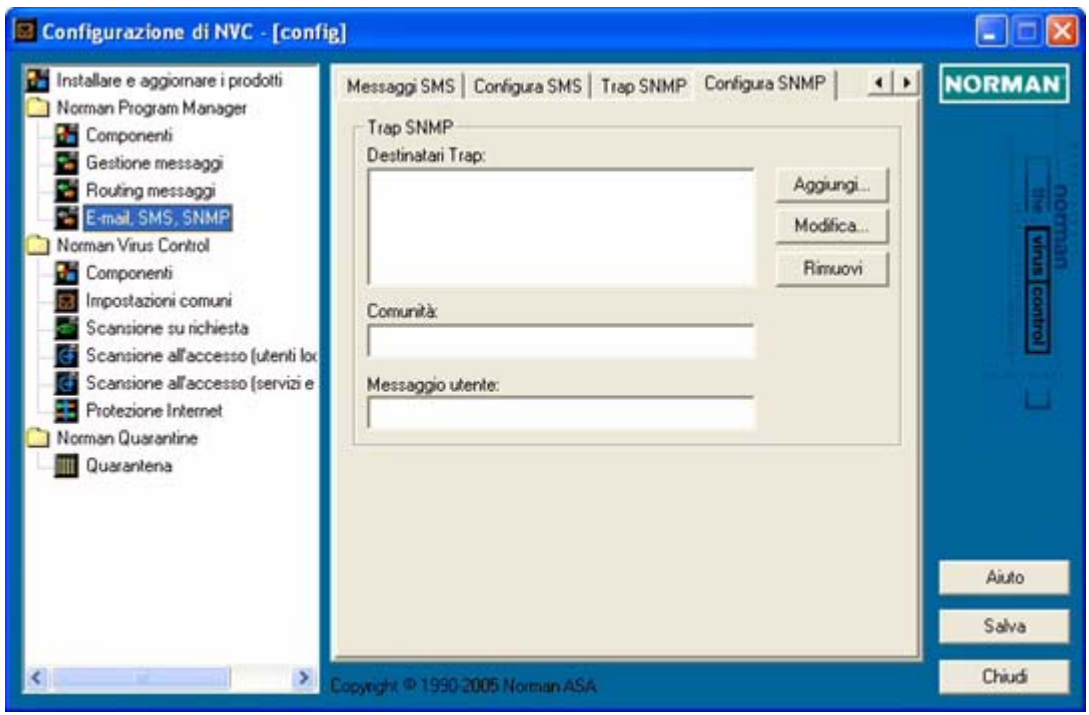
- Fare clic sul pulsante **Aggiungi** per inserire il numero di telefono di un destinatario del messaggio.
- Selezionare una voce dall'elenco e fare clic su **Modifica** per modificare un destinatario esistente.
- Selezionare una voce dall'elenco e fare clic su **Rimuovi** per eliminare un destinatario esistente.

Copyright © 1990-2005 Norman

Testo comune SMS

Si tratta dell'oggetto del messaggio, che apparirà ogni volta che verrà inviato un messaggio. Potrebbe essere una buona idea riportare l'evento che ha causato il messaggio, se era stata scelta solo un'alternativa, ad esempio **Infezioni da virus e altri allarmi**. Questo messaggio può essere, ad esempio, "Call SysAdm". Da notare che la lunghezza massima consentita per il messaggio è di 12 caratteri.

Configura SNMP



Compilare questi campi per abilitare le trap SNMP:

Destinatari Trap

Inserire il nome della macchina o l'indirizzo IP di uno o più destinatari.

Copyright © 1990-2005 Norman

- Fare clic sul pulsante **Aggiungi** per immettere il nome o l'indirizzo di un destinatario SNMP.
- Selezionare una voce dall'elenco e fare clic su **Modifica** per apportare modifiche ad un indirizzo esistente.
- Selezionare una voce dall'elenco e fare clic su **Rimuovi** per eliminare un indirizzo esistente.

Nota: È necessario che i destinatari abbiano installato il MIB di Norman per assicurare una corretta decodifica della trap.

Comunità

Ogni oggetto basato su SNMP, ad esempio una trap, appartiene ad una comunità. L'autenticazione si basa sul nome della comunità scritto in testo comune, che deve essere inserito in questo campo. "Public" è un nome utilizzato frequentemente per le comunità.

Messaggio utente

Questo campo è riservato ad un testo comune, configurabile dall'utente, come ad esempio "Ci sono problemi con...".

Copyright © 1990-2005 Norman

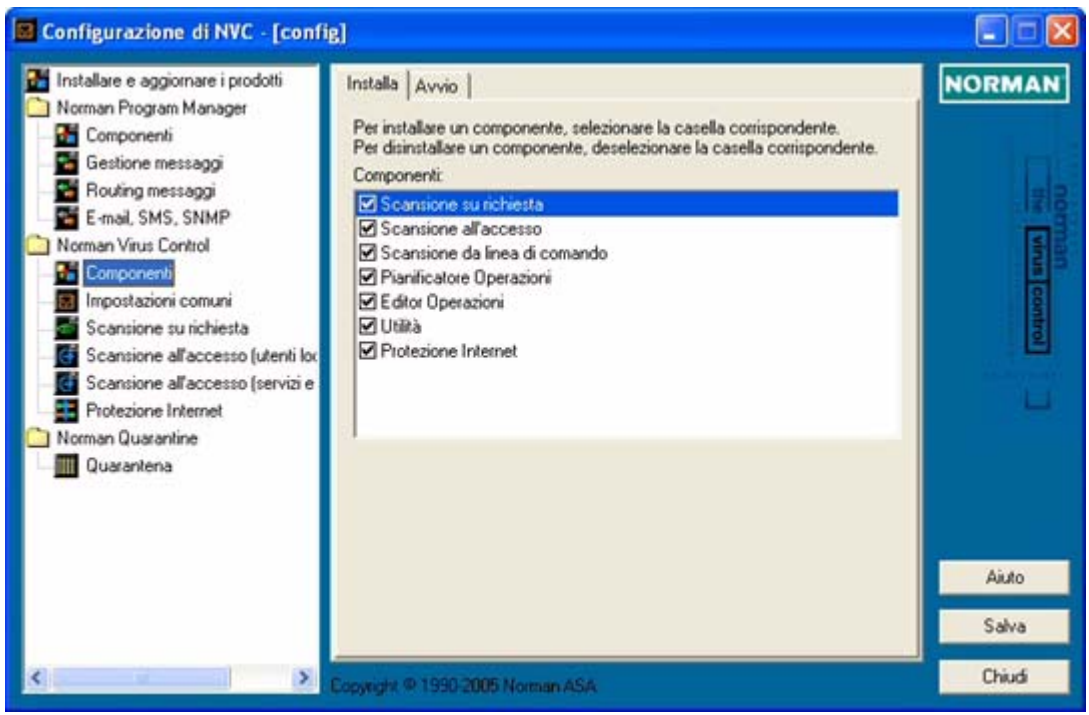
Norman Virus Control

Componenti

Un prodotto quale Norman Virus Control (NVC) include diversi componenti, la cui installazione *completa* risulta vantaggiosa per la maggior parte degli utenti.

Installa

È possibile tornare a questa scheda in qualsiasi momento per aggiungere e/o rimuovere i componenti. Quando viene installato NVC vengono aggiunti tutti i moduli per default.



☑ **Scansionesu richiesta**

La Scansione su richiesta consente di analizzare periodicamente aree selezionate del computer. Se si sta usando il Pianificatore

Copyright © 1990-2005 Norman

Operazioni (vedere sotto), è necessario installare la Scansione su richiesta.

⇨ ‘Scansione su richiesta' a pagina 54.

☑ Scansioneall'accesso

La Scansione all'accesso è un processo che tiene monitorate le attività più importanti del sistema. In base alla configurazione, questo processo può comportare l'accesso ai file e la relativa copia e spostamento in altre unità o directory.

⇨ ‘NVC sui Terminal Server di Windows' a pagina 89.

☑ Scansione da linea di comando

La Scansione da linea di comando è un'alternativa alla scansione eseguita dall'interfaccia utente e offre la possibilità di eseguire dei processi batch e altre operazioni di scansione dalla linea di comando. La Scansione da linea di comando è una valida alternativa per coloro che hanno una buona familiarità con questo ambiente.

⇨ ‘Avvio della scansione da riga di comando' a pagina 109.

☑ Pianificatore operazioni

Il Pianificatore Operazioni è uno strumento che consente di eseguire operazioni ad orari programmati dall'utente.

⇨ ‘Informazioni sul pianificatore' a pagina 97.

☑ Editor Operazioni

Utilizzare questo strumento per creare i file Operazione e per visualizzare/modificare gli eventi immessi nel Pianificatore Operazioni. È possibile inserire un collegamento a un file Operazione sul desktop, sotto forma di icona, o aggiungerlo come voce al menu Start. e devono sempre risiedere nella cartella `...\nvc\tasks`.

In ambiente OS/2 l'ombra dei file Operazione può trovarsi dove desiderato, ma i file veri e propri devono risiedere nella cartella `...\nvc\tasks`.

⇨ ‘Editor Operazioni' a pagina 91.

Copyright © 1990-2005 Norman

☑ **Utilità**

Questo strumento permette di visualizzare e modificare i file Operazione e i file in quarantena, mostra inoltre lo stato dei componenti installati.

⇨ ‘Utilità' a pagina 98.

☑ **Norman Internet protection**

Norman Internet Protection (NIP) è un modulo in grado di intercettare la posta in arrivo e in uscita e di rimuovere o bloccare tutti gli allegati infetti.

Nota: NIP è un modulo per *workstation*. *Non* utilizzare NIP sui server in cui è in esecuzione un servizio SMTP separato o sui terminal server. Su un terminal server NIP protegge *solo* il primo utente che accede al sistema e quindi è inutile in questo tipo di ambiente.
Poiché NIP viene installato come modulo predefinito durante la prima installazione di NVC, anche sui server e sui terminal server, si consiglia di disinstallarlo o disattivarlo su queste piattaforme.

⇨ ‘NVC sui Terminal Server di Windows' a pagina 89.

Avvio

È possibile scegliere di avviare alcuni componenti automaticamente, così che vengano caricati all'avvio del computer. Ci sono tuttavia componenti che per definizione non sono concepiti per un avvio automatico, ad esempio la Scansione su richiesta.

La Scansione all'accesso, al contrario, è stata specificatamente progettata per monitorare il sistema in tempo reale, di conseguenza è per default attivata.

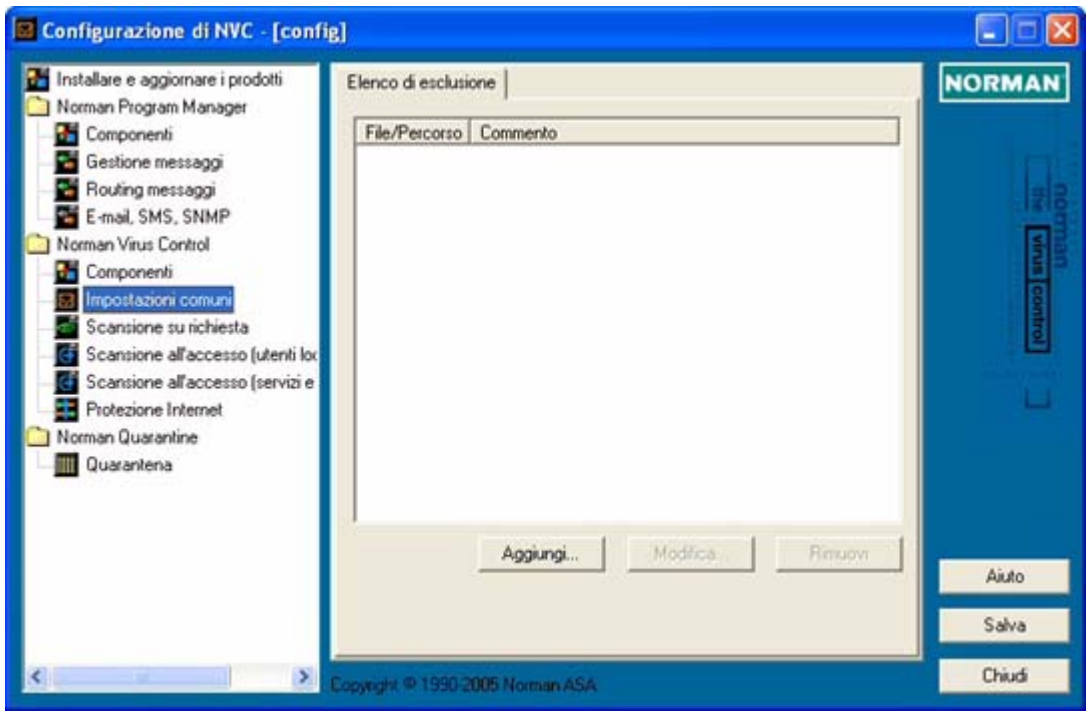
È possibile selezionare anche l'avvio automatico per il Pianificatore Operazioni.

Ogni volta che si modificano le proprietà di un componente, è necessario fare clic su **Salva** per applicare la modifica. Il componente rimane selezionato/deselezionato fino a quando l'utente non lo modifica manualmente e fa clic di nuovo su **Salva**.

Copyright © 1990-2005 Norman

Impostazioni comuni

Le impostazioni comuni riguardano principalmente la gestione del codice dannoso e di conseguenza questo modulo è complementare ai moduli di scansione *Su richiesta* a pagina 54, *All'accesso (utenti locali)* a pagina 89 e *All'accesso a* pagina 63.



Lista di esclusione

Attenzione: gli elenchi di esclusione devono essere gestiti con grande attenzione, poiché rappresentano un potenziale rischio di sicurezza. Si consiglia di analizzare con regolarità la Lista di esclusione manualmente (utilizzando la Scansione su richiesta) ed inoltre di includere questi file o aree nelle scansioni pianificate.

Specificare quali file, directory o unità escludere dalla scansione. Per escludere file dalla scansione seguire le seguenti istruzioni:

Copyright © 1990-2005 Norman

1. Fare clic sul pulsante **Aggiungi** per inserire un file, una directory o la lettera indicante un'unità. È possibile anche utilizzare il pulsante Sfoglia nel campo "File/Percorso da escludere" per selezionare l'oggetto o gli oggetti desiderati. È consentito anche l'uso di caratteri jolly (‘*’ e ‘?’).

   Esempio:

   `c:\dir`

   Esclude tutti i file di questa directory, compreso le sottodirectory.

   `*.xyz`

   Esclude tutti i file con estensione .xyz

   `c:\dir\*.xyz`

   Esclude tutti i file con questa estensioni presenti nella directory.

   `esempio.exe`

   Esclude il file specificato indipendentemente da dove si trova.

   `c:\winnt\system32\xyz.sys`

   Esclude questo file particolare.

   Nota: ***Non*** utilizzare apostrofi o virgolette (' o ") per specificare gli elementi da escludere.

2. Utilizzare il campo **Commento** se si desiderano inserire spiegazioni relative alle varie voci. Poiché è consigliabile rivedere con regolarità la Lista di esclusione, questo campo può tornare utile durante la revisione per ricordarsi il motivo per cui si è escluso dalla scansione un dato elemento.
3. Per modificare una voce esistente, evidenziarla col mouse e fare clic su **Modifica** o **Rimuovi**.
4. Fare clic su **Salva** alla fine dell'operazione.

Scansione su richiesta

La Scansione su richiesta consente di analizzare periodicamente aree selezionate del computer. È possibile avviare la Scansione su richiesta in diversi modi:

Copyright © 1990-2005 Norman

1. Posizionare il cursore su qualsiasi oggetto del file system, ad esempio in Esplora risorse di Windows, fare clic con il pulsante destro del mouse e selezionare NVC dal menu.

⇨ ‘Scansione attivata mediante il pulsante destro del mouse' a pagina 62.

2. Selezionare l'Editor Operazioni dal menu Norman e pianificare l'esecuzione della Scansione su richiesta a una determinata ora o a intervalli di tempo specifici.

⇨ ‘Editor Operazioni' a pagina 91.

3. Utilizzare i collegamenti del menu Norman; **Analizza dischetto** o **Analizza dischi fissi**.

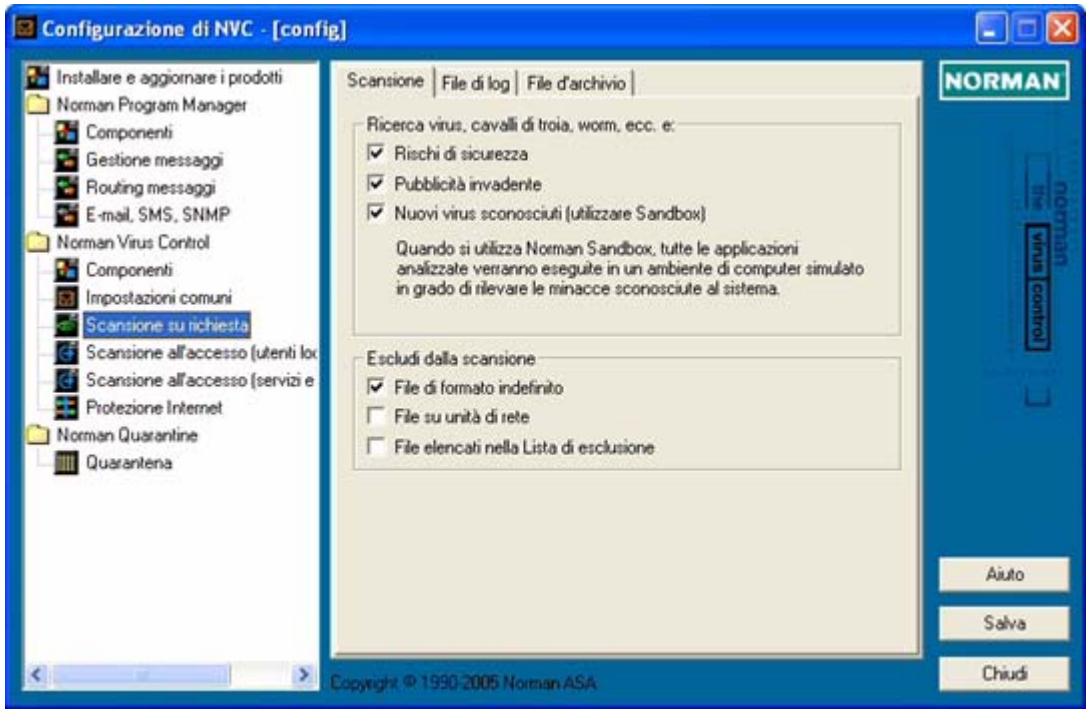
⇨ ‘Collegamento ai moduli NVC e alla scansione' a pagina 14.

Scansione

Per la configurazione di base della Scansione su richiesta fare riferimento alla finestra di dialogo con schede ‘Impostazioni comuni' a pagina 53. Queste impostazioni sono le opzioni di scansione primarie, ovvero quelle utilizzate se si sceglie il valore di default di questa finestra di dialogo.

Questa scheda consente di eseguire temporaneamente una scansione con opzioni diverse.

Copyright © 1990-2005 Norman



Ricerca virus, cavalli di troia, worm, ecc. e:

☑ Rischi di sicurezza

Questa opzione consente di effettuare la scansione alla ricerca di elementi che costituiscono un possibile rischio per la sicurezza. Alcuni amministratori installano programmi come cracker di password e strumenti di amministrazione remota perfettamente legali e probabilmente anche utili. Tuttavia, la mancanza dei necessari requisiti di sicurezza propria di alcuni di essi può esporre il computer all'infiltrazione di cracker e utenti non autorizzati. NVC rileva l'attività di tali programmi avvertendo l'utente del potenziale rischio di sicurezza che rappresentano. Il messaggio segnalerà il nome del programma, così che sia possibile stabilire se l'allarme è stato innescato da un programma legittimo o dall'attività di un cracker.

Copyright © 1990-2005 Norman

☑ Pubblicità invadente

Può trattarsi di quei programmi indesiderati che a volte sono allegati a programmi in versione valutativa scaricati da Internet. La loro presenza non viene rilevata, tanto che anche disinstallando il programma originale possono rimanere nascosti sul computer. Sono difficili da individuare e non hanno alcuna procedura di disinstallazione. Nei momenti più imprevedibili questi programmi iniziano a scaricare pubblicità da Internet. Non sono dannosi come i virus tradizionali, ma sono comunque fastidiosi e creano inutile traffico in rete. NVC rileva e rimuove tali programmi. Selezionando questa opzione, i software freeware installati potrebbero non funzionare.

☑ Nuovi virus sconosciuti che utilizzano Sandbox

La funzione Sandbox di NVC consente di rilevare nuovi virus sconosciuti. Selezionare questa opzione per cercare nuove varianti di virus. Sandbox è particolarmente efficace nella ricerca di nuovi worm e virus di file nei messaggi di posta elettronica, nella rete e in ambienti peer-to-peer; inoltre, reagisce in caso di attacchi alla sicurezza dei sistemi. Quando viene rilevato del nuovo codice dannoso, l'amministratore del sistema riceve tramite il sistema di messaggistica di NVC un messaggio in cui sono elencate le informazioni più importanti. Per un esempio, vedere a pagina 119.

Questa opzione prolunga la durata della scansione ma non ha ripercussioni significative sulle prestazioni. Per ulteriori informazioni su Sandbox, vedere ‘Appendice A - Sandbox' a pagina 117.

Escludi dalla scansione

Per velocizzare il processo di scansione è possibile escludere da esso alcuni file. Bisogna tuttavia tenere presente che escludere file o aree dalla scansione può rappresentare un rischio per la sicurezza.

☑ File di formato indefinito

Selezionare questa opzione se si desidera che NVC tralasci i file in formato indefinito. Possono rientrare in questa definizione file danneggiati o in formato sconosciuto.

Copyright © 1990-2005 Norman

☐ **File su unità di rete**

In ambienti di rete, non tutti gli utenti sono autorizzati ad eseguire la scansione di file residenti sul server. Selezionare questa opzione se si è autorizzati ad effettuare la scansione solo dei file residenti sulla workstation.

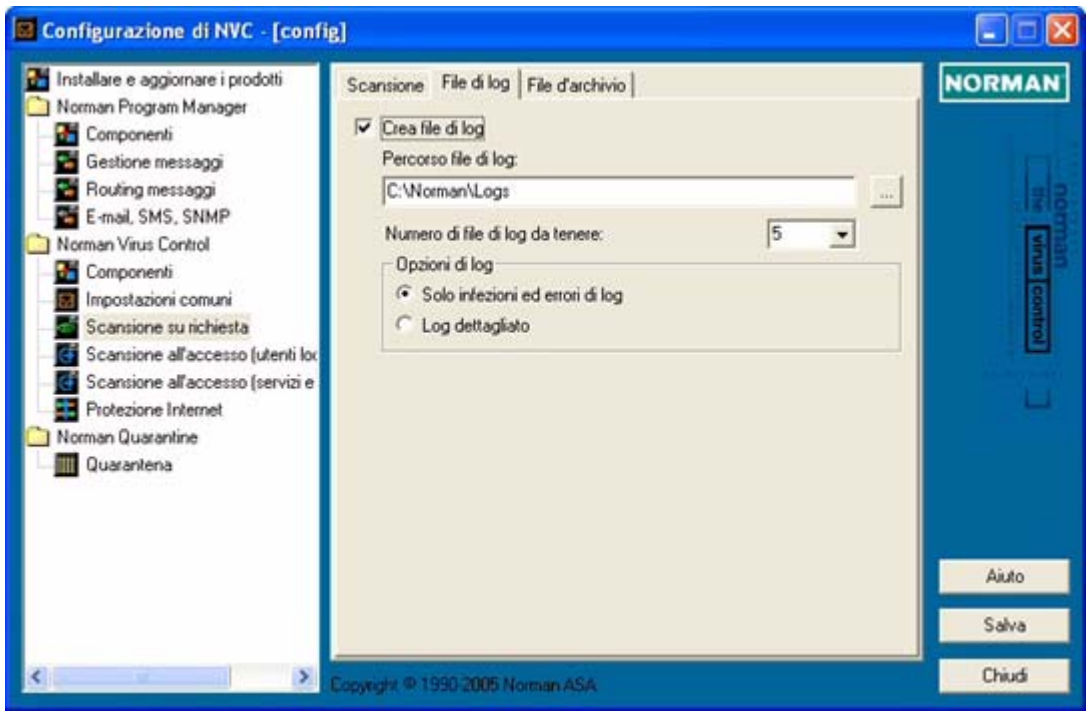
☐ **File elencati nella Lista di esclusione**

Selezionando questa opzione, si attiva la Lista di esclusione. Dato che i file elencati nella Lista di esclusione andrebbero analizzati regolarmente, si consiglia di non selezionare questa opzione.

Copyright © 1990-2005 Norman

file di log

Quando si esegue una scansione manuale NVC genera, per default, un file di log. Il file di log ha un nome e una posizione di default, ed è in grado di presentare un rapporto dettagliato o uno che riporti solo le infezioni e gli errori, a seconda dell'opzione selezionata.



☑ Crea file di log

Crea un file di log ogni volta che si esegue una scansione su richiesta. Deselezionando questa opzione, non verrà generato nessun file di log per le scansioni su richiesta.

Percorso file di log:

Il percorso di default del file di log file è `c:\norman\nvc`. Fare clic sul tasto del browser per specificare un percorso diverso.

Copyright © 1990-2005 Norman

Numero di file di log da tenere:

Selezionando il valore di default 5, si sovrascriverà il file di log più vecchio quando viene generato il file di log numero 6. Il primo file di log viene nominato `nvc00000.log`, seguono `nvc00001.log` , ecc. Similmente, se si tengono 10 file di log, NVC sovrascriverà il primo file di log invece di generare il file di log `nvc00010.log`.

Opzioni di log

⊙ **Solo infezioni ed errori di log**

Si tratta del file di log di default che produce un riepilogo delle aree analizzate, oltre a fornire orario di scansione e numero di file analizzati, dettagli su possibili infezioni ed errori di programma, versione del motore di scansione e data dei file di definizione dei virus.

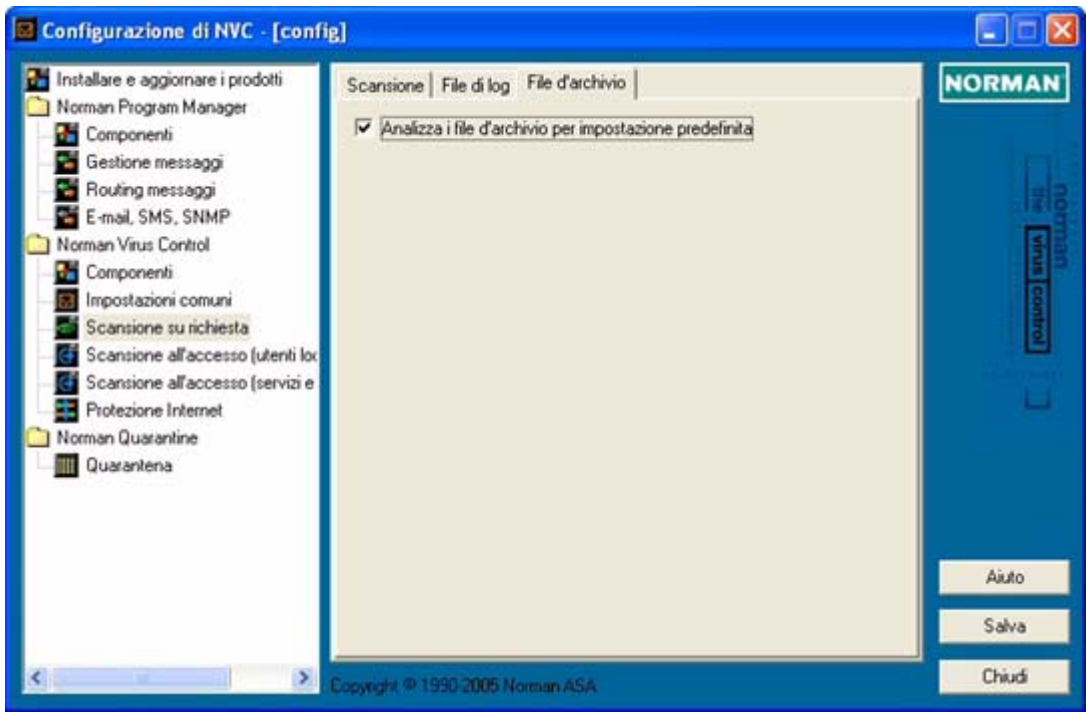
O Log dettagliato

Questa opzione genera un rapporto dettagliatissimo, in cui viene specificato ciascun file analizzato, orario della scansione per file, stato, ecc.

Copyright © 1990-2005 Norman

File d'archivio

I file d'archivio a volte sono di grandi dimensioni e possono contenere un elevato numero di file.



☑ **Analizza i file d'archivio**

NVC è configurato in modo tale che analizzi sempre gli archivi.

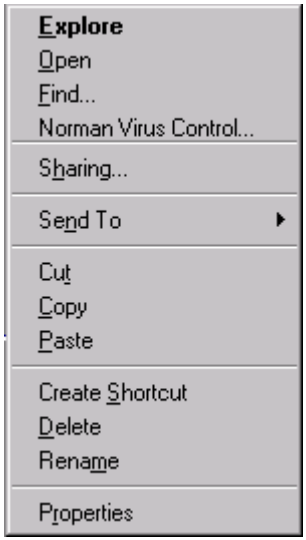
File infetti negli archivi

Se in un archivio viene rilevato un file infetto, NVC cerca innanzitutto di ripararlo. Se non è possibile riparare un file infetto, viene eliminato dall'archivio e il file originale viene messo in quarantena.

La Scansione su richiesta viene eseguita in base alle opzioni di quarantena specificate nel modulo **Quarantena**.

Copyright © 1990-2005 Norman

Scansione attivata mediante il pulsante destro del mouse



Un modo semplice per richiamare la Scansione su richiesta è l'utilizzo del pulsante destro del mouse. Selezionare uno o più oggetti del file system e fare clic con il pulsante destro del mouse per avviare la scansione. Quando si posiziona il cursore sugli oggetti del file system, quali dischi, directory e file, e si fa clic con il pulsante destro del mouse, viene visualizzato un menu di scelta rapida con una voce relativa alla scansione.
Molti utenti considerano la scansione dei virus un male necessario. Se questa operazione diventa facile da eseguire, verrà eseguita sempre più spesso. Per la Scansione su richiesta non è necessario fare doppio clic su un'icona o eseguire un file eseguibile. È sufficiente selezionare l'area o le aree da analizzare in Esplora risorse o dal desktop di OS/2, ad esempio, quindi *Norman Virus Control* dal menu di scelta rapida attivato mediante il pulsante destro del mouse.

La scansione attivata mediante il pulsante destro del mouse utilizzerà le impostazioni specificate in ‘Scansione su richiesta' a pagina 54.

Con la Scansione su richiesta è possibile rilevare e rimuovere automaticamente tutti i tipi di virus, ad eccezione dei virus del settore di boot presenti sulle unità fisse.

⇨ ‘Pulizia dei file infetti' a pagina 110.

Diagnosi

Quando la scansione su richiesta ha completato l'analisi delle aree selezionate, tutte le relative informazioni appaiono nella finestra di dialogo della scansione. Ci sono voci separate per i file infetti e per i file che è stato impossibile analizzare. Nel

Copyright © 1990-2005 Norman

campo ***Diagnosi*** sono riportate le cause che hanno impedito di analizzare un determinato file. La causa più comune è che il file è danneggiato. Un file "danneggiato" non è necessariamente inutile per l'utente, ma NVC non è in grado di riconoscere il formato del file e di conseguenza non analizza il file. Se si verificano altre situazioni meno probabili, si verrà informati del motivo per cui non è stato possibile analizzare un file. Il file di log conterrà ulteriori informazioni a questo proposito.

Scansione all'accesso

La Scansione all'accesso esegue costantemente l'analisi del file system. È fondamentale che un'applicazione antivirus rilevi e blocchi un virus prima che sia attivato. Durante la scansione all'accesso NVC comunica con il sistema operativo ad un livello basso e consente alla scansione di "vedere" tutte le attività in corso sul sistema. In questo modo NVC riesce ad anticipare l'azione del virus e può subito prendere provvedimenti.

Ogni volta che si accede a un file con un'operazione di lettura/scrittura oppure si esegue un programma, viene informata la Scansione all'accesso che analizza automaticamente il file, se è configurata per farlo.

Come la Scansione su richiesta, la Scansione all'accesso di NVC rileva e ripara tutti i tipi di virus. Se possibile, un file infetto viene riparato prima di passare all'applicazione. Se NVC non riesce a ripararlo, nega l'accesso al file infetto.

⇨ ‘Pulizia dei file infetti' a pagina 110.

Scansione all'accesso in Windows NT/2000/XP/2003

Le opzioni di scansione all'accesso per questa piattaforma sono suddivise in due moduli distinti: ***utenti locali*** e ***servizi e utenti remoti***. Normalmente, per le workstation viene utilizzata la modalità utenti locali, mentre per il server viene utilizzata la modalità servizi e utenti remoti. In ogni caso, è necessario configurare i due moduli in modo da contemplare entrambi i ruoli che Windows NT/2000/XP/2003 può assumere. Questi

Copyright © 1990-2005 Norman

ruoli in relazione alla scansione di NVC sono definiti dalle seguenti modalità:

Utenti locali

Controllo antivirus per utenti che hanno effettuato l'accesso, comprensivo di qualsiasi attività in corso sulla macchina locale. Se l'utente è disconnesso o la macchina funge da server, viene applicata la modalità servizi e utenti remoti.

Servizi e utenti remoti

Ogni altra attività eseguita sulla macchina su cui si effettua l'accesso, ad esempio l'accesso da altre macchine a directory condivise. La modalità servizi e utenti remoti viene applicata a qualsiasi computer NT/2000/XP/2003 disconnesso.

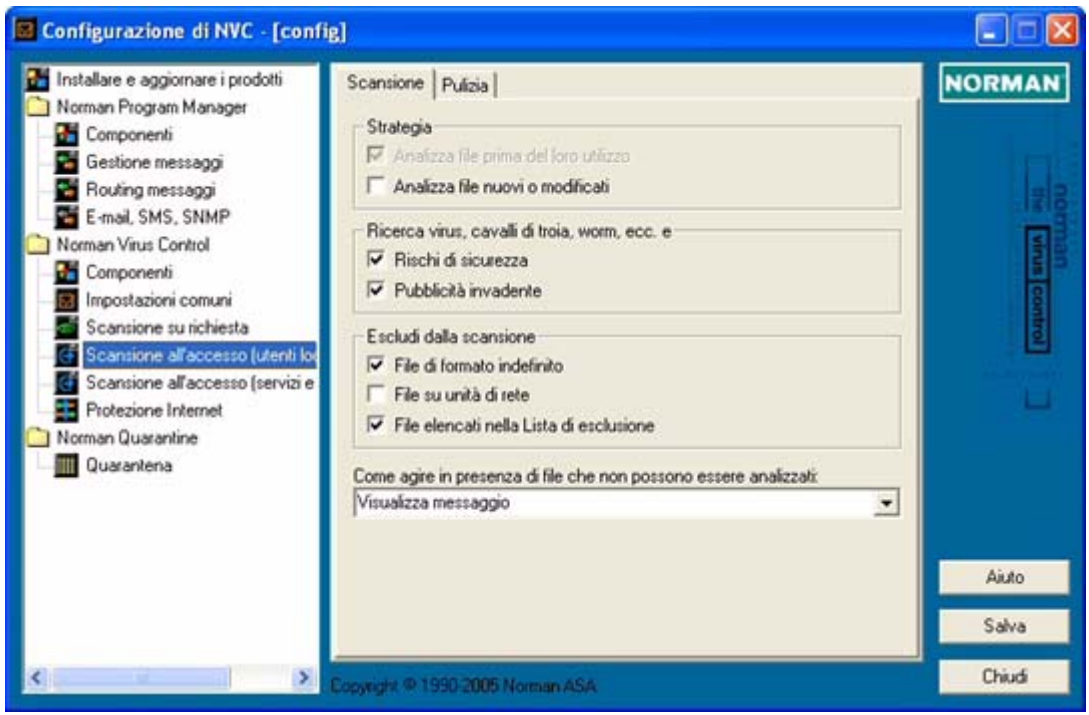
L'attività in modalità servizi e utenti remoti avviene di norma sul server. Se tuttavia si effettua fisicamente l'accesso al server, viene applicata la modalità utenti locali.

Informazioni sulla Scansione all'accesso in Windows 95/98/Me

A differenza della Scansione all'accesso nelle installazioni su Windows NT/2000/XP/2003, la Scansione all'accesso su Windows 95/98/Me è composta da un solo modulo. Questo modulo effettua l'analisi dei file quando un utente connesso accede ai file. Nelle schede della finestra di dialogo di questo modulo di configurazione è possibile modificare le impostazioni della Scansione all'accesso, come ad esempio quali operazioni controllare, quali file escludere dalla scansione e come agire nel caso in cui vengano rilevati dei virus o altro codice dannoso.

Copyright © 1990-2005 Norman

Scansione



Strategia

(valida per Windows 95/98/Me e il modulo "utenti locali" su Windows NT/2000/XP/2003 e OS/2)

In questa sezione è possibile selezionare se si desidera analizzare i file sia prima che vengano utilizzati sia quando vengono creati dei nuovi file o vengono apportate delle modifiche a file già esistenti. In altre parole, si può scegliere una strategia per la scansione all'accesso che si attiva quando un utente si connette localmente al computer.

Queste opzioni si possono considerare come delle impostazioni della "workstation".

Copyright © 1990-2005 Norman

☑ **Analizza file prima del loro utilizzo**

Con questa opzione la Scansione all'accesso analizza i file aperti per essere letti/eseguiti ed è obbligatoria per motivi di sicurezza.

Esempio: Quando si apre un file da un dischetto, un documento dal disco rigido o un allegato di posta elettronica, la Scansione all'accesso analizza automaticamente il file e interviene se rileva del codice infetto. Naturalmente i file di definizione dei virus devono essere aggiornati.

☐ **Analizza file nuovi o modificati**

Con questa opzione la Scansione all'accesso analizza i file aperti per essere scritti, come ad esempio quando si apportano delle modifiche ai documenti o si creano dei nuovi file sul disco rigido.

In Windows NT/2000/XP/2003 il modulo servizi e utenti remoti impedisce ad altri utenti remoti di salvare file infetti sul proprio computer. Nel caso di utenti locali, si consiglia di non utilizzare questa opzione unitamente all'opzione **Analizza file prima del loro utilizzo**, in quanto potrebbe influire negativamente sulle prestazioni del computer e sulle applicazioni che eseguono numerose operazioni di lettura/scrittura.

Si consiglia invece di selezionare questa opzione sui client con sistema operativo Windows 95/98/Me sui quali è abilitata la condivisione di file e/o stampanti.

Strategia

(valida solo per Windows NT/2000/XP/2003 e OS/2)

In questo modulo è possibile selezionare se si desidera eseguire la scansione dei file prima che vengano utilizzati e/o quando vengono creati dei nuovi file, oppure quando vengono modificati dei file già esistenti. In altre parole, si può scegliere una strategia per la scansione all'accesso che si attiva quando altri computer scrivono dei file sul computer/server.

Queste opzioni si possono considerare come delle impostazioni del "server".

☐ **Analizza file prima del loro utilizzo**

Con questa opzione la Scansione all'accesso analizza i file aperti per essere letti/eseguiti.

Copyright © 1990-2005 Norman

Esempio: Se i file che si trovano su una condivisione del server (in cui è selezionata questa opzione) vengono aperti da una workstation, vengono analizzati prima che gli utenti possano accedervi.

Questa opzione prolunga notevolmente la durata della scansione. Pertanto si consiglia di selezionarla sui server solo in caso di infezione da virus diffusa in tutta la rete.

☑ **Analizza file nuovi o modificati**

Con questa opzione la Scansione all'accesso analizza i file aperti per essere scritti, come ad esempio quando gli utenti di una rete salvano il lavoro o creano dei file su un server.

L'opzione predefinita è **Analizza file nuovi o modificati**. Si consiglia di non abbinare questa opzione ad **Analizza file prima del loro utilizzo** a meno che non vi sia un'infezione da virus diffusa in tutta la rete, in quanto rallenta notevolmente le prestazioni.

Importante: Più in particolare, per scansione in scrittura si intende che l'analisi dei file nuovi o modificati avviene nel momento in cui vengono chiusi. Si supponga, ad esempio, che vi sia un computer client non protetto, che è stato infettato da un virus diffuso in tutte le condivisioni della rete. Ogni volta che questo virus infetta un file presente sul server, in cui è stata configurata la Scansione all'accesso per analizzare i file nuovi o modificati, la Scansione all'accesso rileva e rimuove il virus. Purtroppo con i metodi di scansione tradizionali questa operazione avviene *dopo* che il file è già stato infettato. Per i virus come VBS/Loveletter, ciò significa che probabilmente molti file sono già stati danneggiati. Comunque i file vengono inviati in quarantena in modo tale che non siano disponibili agli utenti della rete per non riattivare l'infezione in rete.

Ricerca virus, cavalli di troia, worm, ecc. e

(Valida per tutte le piattaforme supportate)

NVC esegue la scansione alla ricerca di virus, cavalli di troia, worm e altro codice dannoso o di programmi indesiderati che potrebbero danneggiare il PC.

Inoltre è possibile selezionare la scansione per verificare la presenza di:

Copyright © 1990-2005 Norman

☑ Rischi di sicurezza

Questa opzione consente di effettuare la scansione alla ricerca di elementi che costituiscono un possibile rischio per la sicurezza. Alcuni amministratori installano programmi come cracker di password e strumenti di amministrazione remota perfettamente legali e probabilmente anche utili. Tuttavia, la mancanza dei necessari requisiti di sicurezza propria di alcuni di essi può esporre il computer all'infiltrazione di cracker e utenti non autorizzati. NVC rileva l'attività di tali programmi avvertendo l'utente del potenziale rischio di sicurezza che rappresentano. Il messaggio segnalerà il nome del programma, così che sia possibile stabilire se l'allarme è stato innescato da un programma legittimo o dall'attività di un cracker.

☑ Pubblicità invadente

Può trattarsi di quei programmi indesiderati che a volte sono allegati a programmi in versione valutativa scaricati da Internet. La loro presenza non viene rilevata, tanto che anche disinstallando il programma originale possono rimanere nascosti sul computer. Sono difficili da individuare e non hanno alcuna procedura di disinstallazione. Nei momenti più imprevedibili questi programmi iniziano a scaricare pubblicità da Internet. Non sono dannosi come i virus tradizionali, ma sono comunque fastidiosi e creano inutile traffico in rete. NVC rileva e rimuove tali programmi. Selezionando questa opzione, i software freeware installati potrebbero non funzionare.

☑ Rilevamento di nuovi, virus sconosciuti mediante Sandbox

La funzione Sandbox di NVC consente di rilevare nuovi virus sconosciuti. Selezionare questa opzione per cercare nuove varianti di virus. Sandbox è particolarmente efficace nella ricerca di nuovi worm peer-to-peer, nei messaggi di posta elettronica e nella rete e di virus nei file; inoltre reagisce in caso di attacchi alla sicurezza dei sistemi. Quando viene rilevato del nuovo codice dannoso, l'amministratore del sistema riceve tramite il sistema di messaggistica di NVC un messaggio in cui sono elencate le informazioni più importanti. Per un esempio vedere a pagina 119.)

Copyright © 1990-2005 Norman

La selezione di questa opzione è principalmente una protezione aggiuntiva contro worm di rete, ad esempio quando la macchina A è protetta e si tenta di eseguire una copia di codice dannoso su una risorsa condivisa sulla macchina A dalla macchina B.

Nota: L'opzione Sandbox **non** fornisce maggiore protezione per operazioni eseguite dall'utente connesso sulla macchina A. Tali operazioni vengono controllate solo utilizzando file di firma e metodi euristici tradizionali.

Questa opzione prolunga la durata della scansione, ma non ha ripercussioni significative sulle prestazioni. Per ulteriori informazioni su Sandbox, consultare ‘Appendice A - Sandbox' a pagina 117.

Escludi dalla scansione

Per velocizzare il processo di scansione è possibile escludere da esso alcuni file. Bisogna tuttavia tenere presente che escludere file o aree dalla scansione può rappresentare un rischio per la sicurezza.

☑ **File di formato indefinito**

Selezionare questa opzione se si desidera che NVC tralasci i file in formato indefinito. Possono rientrare in questa definizione file danneggiati o in formato sconosciuto.

☐ **File su unità di rete**

Abilitare questa opzione se non si desidera che NVC effettui la scansione delle condivisioni cui si accede su computer remoti.

☑ **File elencati nella Lista di esclusione**

Selezionando questa opzione, i file elencati nella Lista di esclusione non verranno analizzati. Alcuni file non vengono analizzati perché provocano falsi allarmi oppure rallentano la scansione. Comunque si consiglia di analizzare regolarmente i file elencati nella Lista di esclusione eseguendo delle scansioni pianificate o su richiesta,

Copyright © 1990-2005 Norman

Come agire in presenza di file che non possono essere analizzati

(valida per Windows 95/98/Me e il modulo "utenti locali" su Windows NT/2000/XP/2003 e OS/2)

Ci sono situazioni in cui NVC non è in grado di analizzare un file, ad esempio nel caso di documenti Word protetti da password, file danneggiati o errori di sistema interni. NVC offre tre opzioni per gestire i file di cui non è possibile effettuare la scansione. Dal menu a discesa è possibile scegliere tra:

Ignora

NVC non avverte che alcuni file non possono essere analizzati.

Visualizza messaggio

NVC visualizza un messaggio quando si accede a un file per avvertire che quel file non è stato analizzato. Si può comunque procedere a proprio rischio.

Visualizza messaggio e nega l'accesso

NVC avvisa che nega l'accesso al file che non è stato possibile analizzare.

Modalità di scansione all'accesso (NON applicabile su Windows)

☐ **Utilizza modalità di scansione per servizi e utenti remoti**

Quando viene eseguita la scansione all'accesso in modalità utenti locali, vengono visualizzate regolarmente le finestre di dialogo a cui è necessario rispondere. Se è selezionata questa opzione, tali finestre di dialogo non vengono visualizzate sul server e vengono applicate le opzioni di configurazione della scansione servizi e utenti remoti.

Questa opzione è valida solo per le reti con server OS/2.

Per ambienti di rete:

Il campo Accesso nella parte inferiore di tutte le schede viene visualizzato solo se si dispone dei diritti di amministratore. L'amministratore del sistema stabilisce gli elementi da rendere visibili e/o configurabili dalle workstation. L'utente normale può pertanto vedere tutte o alcune delle schede, ma può non essere autorizzato a modificare le impostazioni.

Copyright © 1990-2005 Norman

Pulizia

NVC permette di scegliere come agire nei confronti di eventuali virus, cavalli di troia, worm o altro codice dannoso.

Nega l'accesso

Se si tenta di eseguire un programma infetto, l'accesso viene negato. I documenti infetti vengono bloccati.

Nota: Per la Scansione all'accesso (servizi e utenti remoti), questa opzione è importante solo se è stata selezionata la strategia di scansione **Analizza file prima del loro utilizzo**. In altre parole, se si utilizzano le impostazioni predefinite, si consiglia di **non** selezionare questa opzione.

Rimuovi

NVC cercherà di rimuovere il virus dal file infetto. Selezionare questa opzione se si desidera che NVC ripari automaticamente i file infetti. NVC è in grado di rimuovere automaticamente la maggioranza dei virus, ad eccezione dei virus del settore di boot. NVC interpella sempre l'utente prima di rimuovere virus dal settore di boot. Si noti che un file infetto viene completamente eliminato nel caso sia costituito esclusivamente da codice dannoso e non da altre informazioni.

Chiedi all'utente

Selezionare questa opzione se non si desidera la rimozione automatica dei virus né l'accesso negato ai file infetti. Quando si cercherà di accedere ad un file infetto, si riceverà un messaggio che avverte dell'infezione e dalla finestra visualizzata sarà possibile scegliere se rimuovere il file o uscire.

Consigli:

- Assicurarsi che la propria installazione di NVC sia aggiornata. È la migliore protezione dagli attacchi dei virus in quanto è possibile bloccare i virus prima che entrino nel sistema.
- Installare il software antivirus sui server di posta elettronica e sui gateway.
- Limitare il più possibile i diritti degli utenti sulle condivisioni, ad esempio impostando, se possibile,

Copyright © 1990-2005 Norman

l'attributo di sola lettura sui file che non vengono modificati di frequente.

- Eseguire regolarmente delle copie di riserva dei file.

Scansione all'accesso nelle reti

NVC esegue di default la scansione dei file a cui si accede sulle unità di rete. Quando i file da analizzare risiedono sulle unità di rete, il comportamento della Scansione all'accesso dipende dai diritti dell'utente connesso. Quando la Scansione all'accesso vede un file aperto da un'unità di rete, analizza come al solito il file. Tuttavia non può riparare, rimuovere o inviare in quarantena un file infetto se l'utente connesso non ha accesso in scrittura alla directory/file in questione. Inoltre gli verrà negato l'accesso al file infetto.

Detto ciò, non si significa che occorre essere meno restrittivi con i privilegi degli utenti. Se una Scansione all'accesso aggiornata protegge sia i server che i client, è improbabile che la Scansione all'accesso sui client rilevi del codice dannoso nelle unità di rete. Tuttavia, se si dovesse verificare questa situazione, ci si può difendere.

Quando la Scansione all'accesso rileva dei virus o altro codice dannose sulle unità di rete, visualizza la posizione sotto forma di percorsi UNC e unità non connesse. Molti utenti conoscono le unità di rete come X, Y, Z, ecc. Il messaggio di avvertimento visualizzato dalla Scansione all'accesso è, ad esempio `\\Server\Share\InfectedFile` anziché `X:\Infected file`.

La scansione all'accesso nelle reti viene eseguita solo sui server senza controllo dei virus, semplicemente per evitare che gli stessi file vengano sottoposti a scansione due volte, la prima volta sul server e di nuovo quando vengono aperti sul client. La conseguenza della doppia scansione potrebbe essere un rallentamento dei logon alla rete e dei backup. Tuttavia la decisione finale spetta ai singoli amministratori del sistema in quanto la sicurezza del sistema da un lato e il funzionamento della rete dall’altro sono entrambi fattori importanti da tenere in considerazione.

Copyright © 1990-2005 Norman

È possibile disattivare la Scansione all'accesso per i file in rete selezionando l'opzione "Escludi dalla scansione" di **File su unità di rete**.

Norman Internet Protection

Nota: La versione corrente di Norman Internet Protection è solo per la piattaforma Windows e *non* funziona con OS/2.

Norman Internet Protection (NIP) è un filtro proxy che protegge dai virus che si diffondono tramite

- posta Internet
- lettori di news

La maggior parte dei virus segnalati ad oggi utilizza dei meccanismi che ne consentono la diffusione tramite posta elettronica. È statisticamente dimostrato che un messaggio di posta elettronica su 30 inviato durante un'epidemia di virus contiene del codice in qualche modo dannoso. È quindi indispensabile proteggersi dagli attacchi di virus.

NIP è un modulo di NVC 5 in grado di intercettare la posta in arrivo e in uscita e le news e di rimuovere o bloccare tutti gli allegati infetti.

NIP è in grado sia di analizzare messaggi di posta elettronica alla ricerca di virus sconosciuti sia di bloccare gli allegati, in base al contenuto e all'estensione.

Dato che è un componente integrato di NVC 5, può essere distribuito tramite la rete e pertanto costituisce un'ulteriore barriera per fronteggiare i continui attacchi dei virus provenienti "dall'esterno".

Limitazioni importanti:

La versione corrente di NIP è più adatta agli utenti privati che agli ambienti professionali. Attualmente, si tratta più di una workstation che di un modulo per server, in parte in quanto NIP non analizza i server di posta locali alla ricerca di codice infetto.

Copyright © 1990-2005 Norman

Definizioni

Lettori di news

Un **lettore di news** è un'applicazione che consente di leggere i messaggi inviati ai newsgroup Internet e di inviare i propri messaggi. I browser più diffusi, quali *Internet Explorer* e *Netscape*, hanno un proprio lettore di news e sono anche disponibili numerosi lettori di news autonomi.

Winsock

Winsock, che è l'abbreviazione di *Windows Socket*, è un'interfaccia di programmazione e il programma di supporto che gestisce le richieste di input/output per le applicazioni Internet in Windows. Ciascuna versione di Windows dispone di una propria versione di `winsock.dll`. In parole semplici, Winsock è il "ponte" tra i programmi Windows e le connessioni TCP/IP (Internet).

È importante tenere presente che altri fornitori offrono versioni freeware e shareware di `winsock.dll` che **non** seguono gli standard di Microsoft. Queste versioni possono differire per dettagli minori. Questo non costituisce un vantaggio per l'utente o per i programmatori di terze parti di applicazioni Internet per la piattaforma Windows.

Nota: Tutti i prodotti Norman che fanno uso di `winsock.dll` sono conformi agli standard di Microsoft.

Protocollo

Un **protocollo** è un formato definito per la trasmissione di dati tra due periferiche. Si può considerare come un linguaggio: l'utente deve solo preoccuparsi che la macchina supporti gli stessi protocolli quando comunica con altri computer.

La versione corrente di NIP supporta questi **protocolli**:

- POP3, per la posta in arrivo;
- SMTP, per la posta in uscita;
- NNTP, per i newsgroup.

Copyright © 1990-2005 Norman

Porta

Una porta è un "punto di connessione logica" nella programmazione e, nello specifico, se si utilizza il protocollo TCP/IP di Internet, il modo in cui un programma client specifica un particolare programma server su un computer in rete. Le applicazioni che utilizzano TCP/IP, come il protocollo Web HTTP, hanno porte con numeri preassegnati. Tali porte sono denominate "porte conosciute" assegnate da un comitato internazionale ufficiale (IANA). Ai processi di altre applicazioni vengono assegnati i numeri di porta in modo dinamico per ogni connessione. La prima volta che viene avviato un servizio (programma server), viene detto che tale servizio esegue il binding al relativo numero di porta designato. Poiché tutti i programmi client desiderano utilizzare il server, anche tali programmi devono richiedere il binding al numero di porta designato.

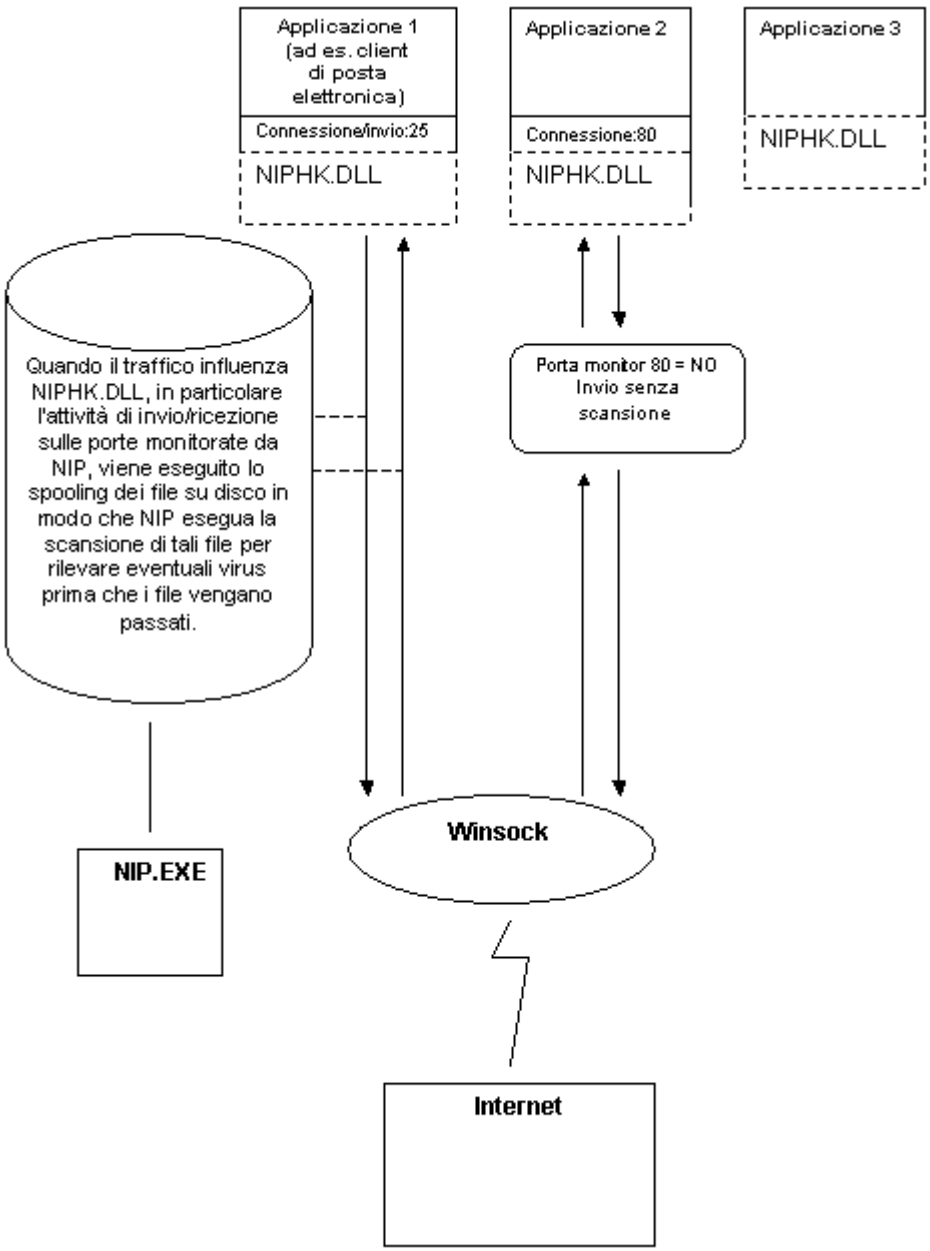
I numeri di porta sono compresi tra 0 e 65536. Le porte da 0 a 1024 sono riservate a determinati servizi privilegiati. Per il servizio HTTP, la porta 80 è quella predefinita e non è necessario specificarla nell'URL (Uniform Resource Locator).

Fare riferimento alla sezione ‘Avanzate' a pagina 85 e alle sezioni successive per una panoramica dei protocolli supportati di NIP e dei corrispondenti numeri di porta.

Come dimostrano queste definizioni, l'interconnessione tra i protocolli, le porte e gli standard differenti rappresentano un possibile rischio di "conflitto di interessi".

Copyright © 1990-2005 Norman

Come funziona


Applicazione 1 (ad es. client di posta elettronica)
Connessione/invio:25
NIPHK.DLL
Applicazione 2
Connessione:80
NIPHK.DLL
Applicazione 3
NIPHK.DLL
Quando il traffico influenza NIPHK.DLL, in particolare l'attività di invio/ricezione sulle porte monitorate da NIP, viene eseguito lo spooling dei file su disco in modo che NIP esegua la scansione di tali file per rilevare eventuali virus prima che i file vengano passati.
Porta monitor 80 = NO Invio senza scansione
NIP.EXE
Winsock
Internet

Copyright © 1990-2005 Norman

La DLL (*Dynamic Link Library*) `niphk.dll` viene inserita in tutte le applicazioni in esecuzione ed è in grado di monitorare/sottoporre a scansione tutto il traffico Winsock. Winsock, illustrato a pagina 74, gestisce le richieste di input/output delle applicazioni Internet sulla piattaforma Windows.

La versione corrente di NIP supporta tre protocolli: POP3 (posta in arrivo), SMTP (posta in uscita) ed NNTP (newsgroup).

Ogni volta in cui `niphk.dll` rileva un'operazione che utilizza uno di questi protocolli, richiama `nip.exe` per la scansione. Si supponga, ad esempio, di avere posta in arrivo con allegati sulla porta 110. NIP *esegue lo spooling* (memorizzazione temporanea) sull'unità fissa sulla quale viene eseguita la scansione. Tuttavia, se NIP non è configurato per il monitoraggio della posta in arrivo sulla porta 110, ignorerà qualsiasi attività che ha luogo su tale porta.

NIP fa riferimento alle porte standard per il traffico di cui esegue il monitoraggio. Se sono state installate altre applicazioni che utilizzano porte differenti per lo stesso tipo di traffico, potrebbe essere necessario configurare determinate impostazioni che riflettano questa condizione.

Attivazione di NIP

Nota: I diritti definiti in `default.ndf` specificano quali sono le modifiche che un utente può apportare all'installazione locale.

Per installare questo modulo, accedere alla scheda **Installa** nella cartella del prodotto **Norman Virus Control|Componenti** nell'Editor di Configurazione (vedere pagina 50). Selezionare ***Norman Internet Protection*** dall'elenco e fare clic su **Salva**.

Dopo alcuni istanti viene visualizzata la voce ***Norman Internet Protection*** nella scheda **Avvio**. Selezionarla di nuovo e fare clic su **Salva**.

È possibile che sia necessario uscire e riavviare l'Editor di Configurazione per accedere alle opzioni di configurazione NIP.

Per interrompere il NIP, deselezionare la casella di controllo e fare clic su **Salva**.

Copyright © 1990-2005 Norman

Scansione dei virus

I file scaricati, prima di essere passati agli utenti, vengono memorizzati temporaneamente sul disco rigido del client per controllare se sono presenti eventuali virus.

NVC cerca di pulire i file infetti prima che vengano eliminati o messi in quarantena. A volte pulire significa eliminare, come ad esempio nel caso dei *cavalli di troia* in quanto tutto il file è costituito da codice dannoso.

Nota: Per default, una copia del file eliminato o bloccato viene messa in quarantena.

Sostituzione del contenuto nei messaggi di posta elettronica

Quando al client di posta viene notificato un nuovo messaggio ed NVC lo elimina in quanto infetto, il programma di posta elettronica reagisce al mancato arrivo del messaggio segnalato. Pertanto, NVC inoltra eventuali messaggi di posta elettronica sottoposti alla pulizia da contenuto infetto. È comunque possibile visualizzare il mittente del messaggio inviato in origine con una spiegazione.

NVC, ad esempio, ha pulito un file di Word allegato prima che il messaggio fosse accettato dal destinatario. È possibile che nella parte superiore del corpo del messaggio venga visualizzato un messaggio

per indicare che Norman Virus Control ha pulito l'allegato Inventory.doc in quanto conteneva il virus W97M/Claud.A.

Se viene rilevato altro codice infetto, viene visualizzato testo simile nelle relative informazioni.

Nota: NON confondere tale messaggio con avvisi e-mail ricevuti da altri software antivirus per indicare che sul computer di sta diffondendo un virus. Il testo di sostituzione di NVC dimostra semplicemente che NVC ha eseguito il lavoro e non sono presenti problemi.

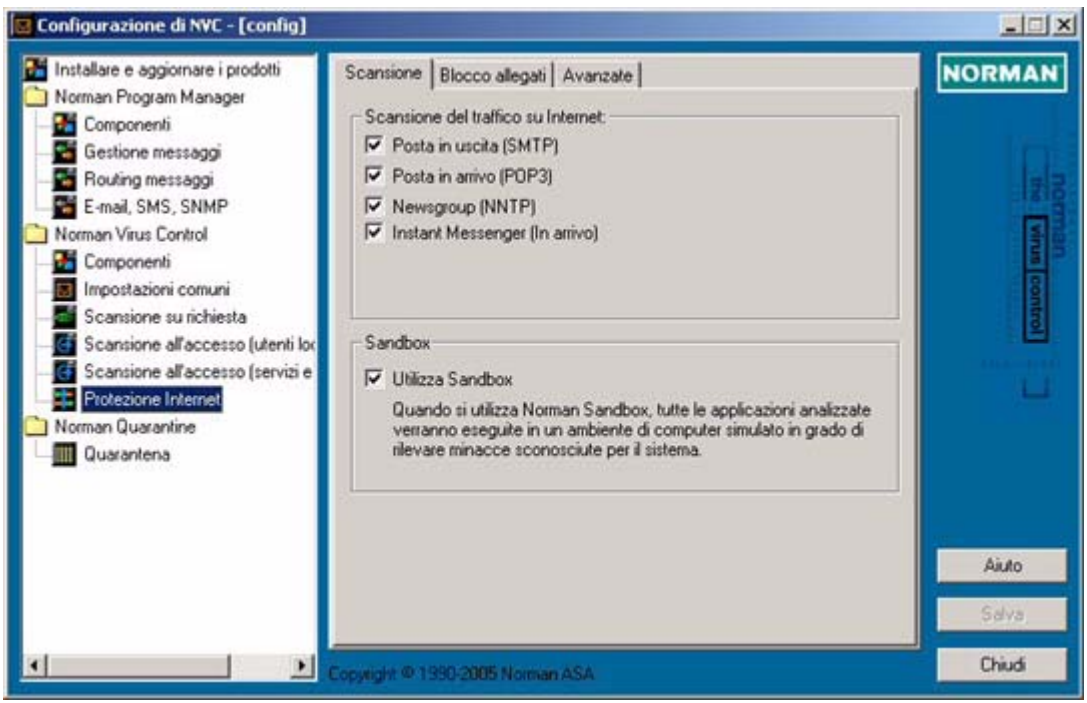
In questo modo il programma di posta elettronica riceve il messaggio atteso, mentre l'utente può verificare che NVC abbia eseguito il lavoro ed eliminato il contenuto infetto.

Copyright © 1990-2005 Norman

Configurazione del NIP

NIP è costituito da tre finestre di dialogo in cui è possibile selezionare gli elementi da sottoporre a scansione, bloccare gli allegati in modo generico o specifico, inviare messaggi di avvertimento in caso di rilevamento di virus e definire i numeri di porta per i protocolli corrispondenti.

Scansione



Selezionare gli elementi del traffico Internet da includere nella scansione. Per default viene effettuata la scansione di tutti gli elementi.

Scansione del traffico su Internet

☑ Posta in uscita (SMTP)

Effettua la scansione di tutti i messaggi di posta elettronica inviati dal sistema. Se ad esempio la macchina è stata

Copyright © 1990-2005 Norman

colpita da virus di cui non si è consapevoli, i messaggi inviati ad amici e collaboratori potrebbero essere infetti.

☑ Posta in arrivo (POP3)

Effettua la scansione di tutti i messaggi di posta elettronica ricevuti. Anche in questo caso la posta inviata persino dall'amico più caro o dal collaboratore più fidato potrebbe inconsapevolmente contenere un virus.

☑ Newsgroup (NNTP)

Effettua la scansione del traffico generato tra il computer dell'utente e quelli di altri partecipanti del gruppo/forum.

⇨ Consultare ‘Definizioni' a pagina 74 per ulteriori informazioni su questo argomento.

☑ Instant Messenger (In arrivo)

Scansione del traffico rappresentato dal trasferimento di file durante le sessioni di messaggistica istantanea con MSN Messenger e Windows Messenger. Quando questa opzione è selezionata, NIP esegue la scansione dei file in arrivo per rilevare eventuale codice dannoso. Se un file risulta infetto, viene visualizzato un messaggio popup per informare l'utente dell'evento.

Vengono analizzati solo i trasferimenti di file, pertanto, i collegamenti infetti rappresentano ancora una minaccia.

Tenere presente che i file trasferiti vengono analizzati quando vengono scritti nella directory `...\Temporary Internet Files`. Se viene rilevato codice dannoso, è probabile che venga messo in quarantena un file .tmp. Per ripristinare il file .tmp in quarantena, selezionare il file desiderato, scegliere l'opzione **Salva con nome** dal menu visualizzato con il pulsante destro del mouse e salvare il file con il nome e l'estensione originali.

⇨ Consultare ‘Quarantena' a pagina 87.

Sandbox

☑ Utilizza Sandbox

La funzione Sandbox di NVC consente di rilevare nuovi virus sconosciuti. Selezionare questa opzione per cercare nuove varianti di virus. Sandbox è particolarmente efficace nella ricerca

Copyright © 1990-2005 Norman

di nuovi worm e virus di file nei messaggi di posta elettronica, nella rete e in ambienti peer-to-peer; inoltre, reagisce in caso di attacchi alla sicurezza dei sistemi. Quando viene rilevato del nuovo codice dannoso, l'amministratore del sistema riceve tramite il sistema di messaggistica di NVC un messaggio in cui sono elencate le informazioni più importanti. Per un esempio, vedere a pagina 119.

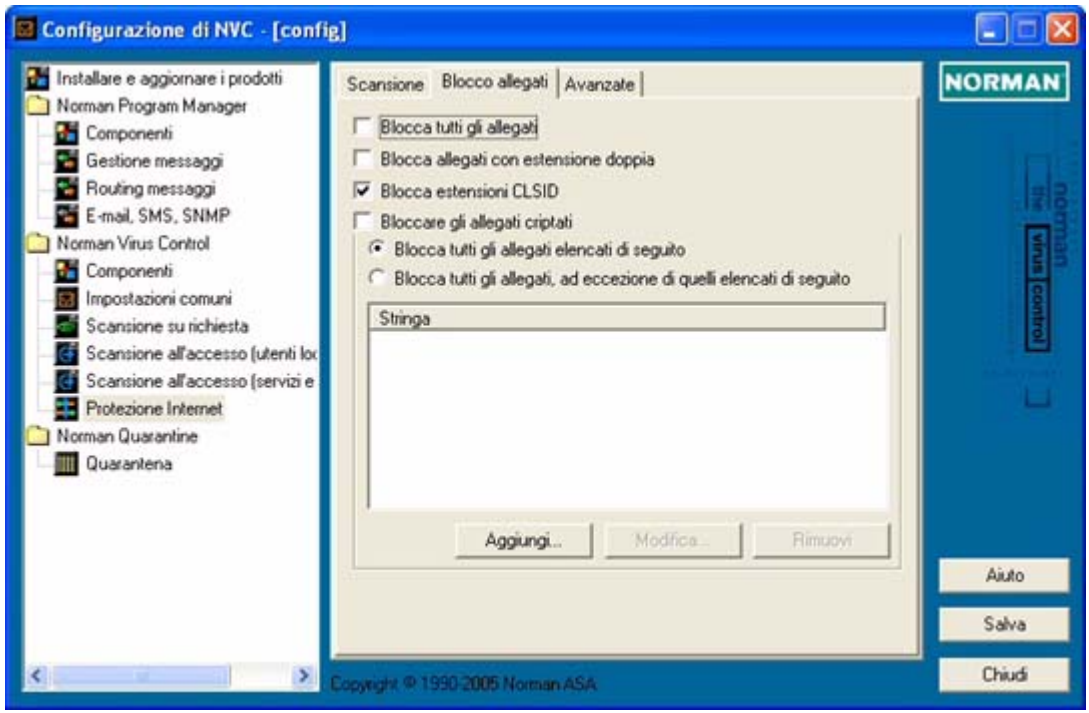
Questa opzione prolunga la durata della scansione ma non ha ripercussioni significative sulle prestazioni. Per ulteriori informazioni su Sandbox, vedere ‘Appendice A - Sandbox' a pagina 117.

Blocco degli allegati

Per bloccare gli allegati è possibile, ad esempio, immettere il nome di un file specifico oppure di file con una certa estensione. Questa funzione risulta particolarmente utile quando sono in circolazione dei worm di posta elettronica che è possibile identificare in base al nome. Il blocco degli allegati è utile anche per fermare dei tipi di file che non si desidera ricevere nella propria casella di posta.

Un allegato bloccato viene *spostato* nell'area destinata alla quarantena ma non viene *eliminato*. In questo modo, è possibile disporre di un backup del file nel caso in cui questo non sia infetto. Una volta messo in quarantena, il file non può arrecare alcun danno. Se, ad esempio, l'utente ha specificato che tutti gli eseguibili (*.exe) devono essere bloccati, può essere rassicurante sapere che è possibile recuperare un file necessario.

Copyright © 1990-2005 Norman



☐ **Blocca tutti gli allegati**

Vengono bloccati tutti gli allegati.

☐ **Blocca qualsiasi allegato con estensione doppia**

Molti worm e virus di posta elettronica applicano una tecnica che prevede l'aggiunta di un'estensione aggiuntiva, ad esempio `<filename>.jpg.vbs`. La maggior parte dei client di posta elettronica nasconde l'ultima estensione e l'allegato sembrerà avere soltanto l'estensione .jpg. Tuttavia, questa funzione non è utilizzata solo dai virus. File provenienti da una fonte sicura con nomi quali `file.hlp.zip` e `elenco_attività 20.dec.doc` vengono considerati come file con estensione doppia.

☑ **Blocca estensioni CLSID**

Alcuni worm e virus di posta elettronica recenti applicano la tecnica CLSID per confondere i motori di scansione della posta elettronica e bloccare il software. Sfruttano infatti una funzione

Copyright © 1990-2005 Norman

di Windows che consente di sostituire un'estensione .exe con un'estensione {...} per sfuggire al blocco dei file .exe. Poiché tale tipo di estensione non viene utilizzato per allegati che provengono da una fonte sicura, questi file vengono automaticamente bloccati.

☐ **Blocca allegati crittografati**

In base agli strumenti utilizzati, è in genere più difficile ricercare i virus negli allegati compressi e crittografati che nei file normali. Pertanto, NIP consente di bloccare completamente tali allegati.

Elenco allegati

Utilizzare questa funzione per selezionare esplicitamente gli allegati che si desidera bloccare o certificare. È possibile immettere il nome esatto di un allegato oppure utilizzare il carattere jolly ('*') per bloccare estensioni specifiche. Ad esempio, per bloccare tutti i file `.exe`, fare clic su **Aggiungi** e immettere `*.exe`. Quando si fa clic su **OK**, la voce appare nella casella di riepilogo, da cui può essere modificata o rimossa in un secondo momento.

⊙ **Blocca tutti gli allegati elencati di seguito**

Tutti i nomi aggiunti all'elenco, utilizzando **Aggiungi**, vengono *bloccati*. Immettere un nome specifico oppure utilizzare il carattere jolly ('*') per identificare gli allegati da bloccare.

O Blocca tutti gli allegati, ad eccezione di quelli elencati di seguito

Tutti i nomi aggiunti all'elenco, utilizzando **Aggiungi**, vengono *accettati*. Immettere un nome specifico oppure utilizzare il carattere jolly ('*') per identificare gli allegati da accettare.

Nota: È *molto* importante distinguere queste due opzioni, perché rappresentano due estremi: *bloccare* tutto ciò che è riportato nell'elenco o *accettare* tutto ciò che è riportato nell'elenco.

Consigli

Gli elenchi di estensioni riportati di seguito non sono statici e verranno aggiornati per far fronte agli attacchi dei principali

Copyright © 1990-2005 Norman

virus e codici dannosi. Per utilizzare questi consigli, selezionare ⊙ **Blocca tutti gli allegati elencati di seguito**.

Livello di sicurezza: Medio

Aggiungere le seguenti estensioni all'elenco dei file che si desidera bloccare:

*.BAT	*.CHM	*.CMD	*.COM	*.CPL
*.EXE	*.HLP	*.HTA	*.HTM	*.INF
*.JS	*.JSE	*.LNK	*.MSI	*.PIF
*.REG	*.SCR	*.SHS	*.SWF	*.VBE
*.VBS	*.WSC	*.WSH	*.URL	*.PL
*.SH	*.CLA	*.PI	*.DLL	

Livello di sicurezza: Elevato

Selezionare l'opzione ***Blocca tutti gli allegati, ad eccezione di quelli elencati di seguito***. Se si sceglie un livello di protezione elevato, prestare attenzione quando si utilizza la funzione **Aggiungi** per elencare i tipi di file accettati. È infatti consigliabile aggiungere a tale elenco i tipi di file ricevuti o scambiati con maggior frequenza.

Nota: Tenere presente che una copia dell'allegato bloccato viene messa in quarantena e *non* viene eliminata, pertanto è possibile ripristinare un file bloccato per errore.

Nel caso in cui si desideri, ad esempio, scambiare tramite posta elettronica dei file *.exe non infetti senza che vengano bloccati da NIP, è necessario crittografarli oppure scambiarli in un formato compresso, come ad esempio *.zip.

Stringa

In questo campo è possibile specificare i nomi da bloccare. È ammesso l'uso del carattere jolly ('*') per bloccare le estensioni specificate. Per ovvi motivi, è possibile usare il carattere jolly solo per i nomi dei file, ad esempio `*.vbs`. Per la maggior parte degli utenti i tipi di file `.vbs`, `.pif` o `..lnk` sono estremamente critici. Inoltre si consiglia di bloccare le estensioni/tipi di file quali `.exe`, `.com` e `.bat` in quanto costituiscono un rischio potenziale per infezioni da virus.

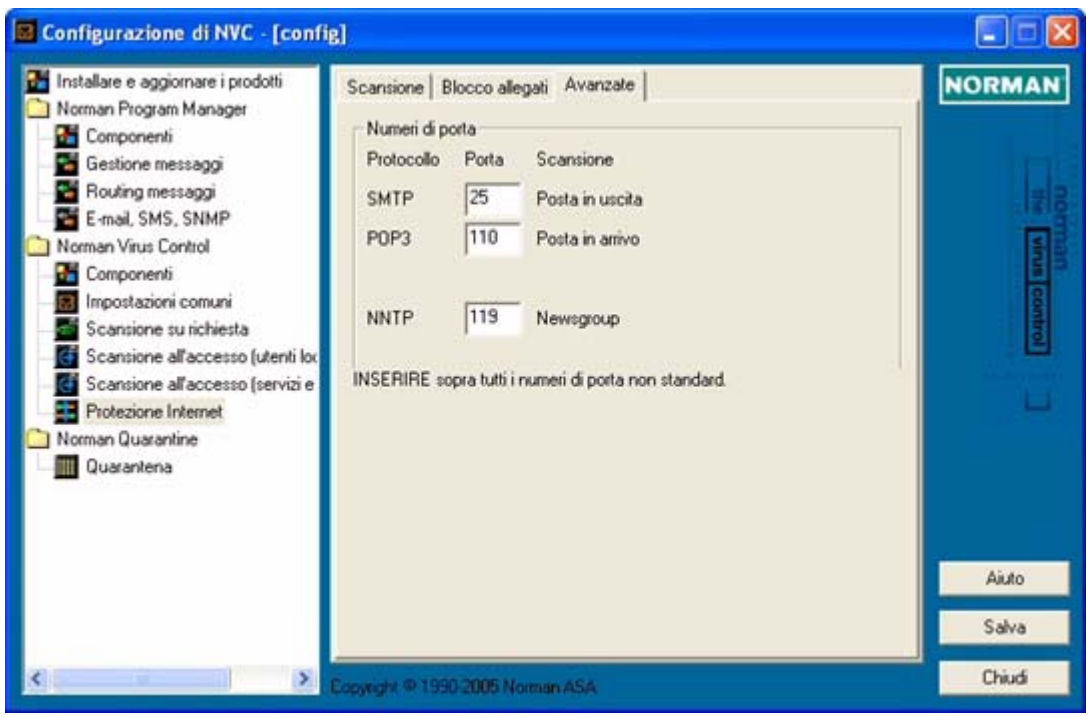
Copyright © 1990-2005 Norman

In questo campo è inoltre possibile bloccare allegati specifici con nomi che notoriamente contengono virus, come `AnnaKournikova.jpg.vbs`. In teoria, è possibile bloccare un virus prima che il fornitore renda disponibili i file di definizione dei virus aggiornati.

Nota: Anche in Outlook 2002 è disponibile una funzione di blocco che viene applicata *dopo* che gli allegati hanno superato il controllo di NIP.

Avanzate

Tra i numerosi protocolli per comunicazione tra computer alcuni sono essenziali per l'utilizzo di Internet. Per motivi di standardizzazione ai protocolli vengono preassegnati numeri di porta.



Copyright © 1990-2005 Norman

Numeri di porta

Nella finestra di dialogo **Scansione** a pagina 79 è stato selezionato il traffico Internet di cui effettuare la scansione. In questa finestra di dialogo vengono identificati i protocolli necessari per l'invio e la ricezione di messaggi di posta elettronica, ad esempio, e il numero di porta corrispondente sul PC, in base agli standard del settore.

È possibile assegnare numeri di porta diversi a uno o più dei protocolli supportati elencati. In tal caso, è necessario immettere il numero di porta ***effettivo*** per i protocolli interessati.

Attualmente sono supportati i protocolli riportati di seguito. È probabile che l'elenco venga aggiornato qualora necessario.

Vengono riportati i nomi completi unitamente ai nomi abbreviati. I numeri di porta e le funzioni sono già specificate nella finestra di dialogo:

• **SMTP** (porta 25) è l'abbreviazione di *Simple Mail Transport Protocol*

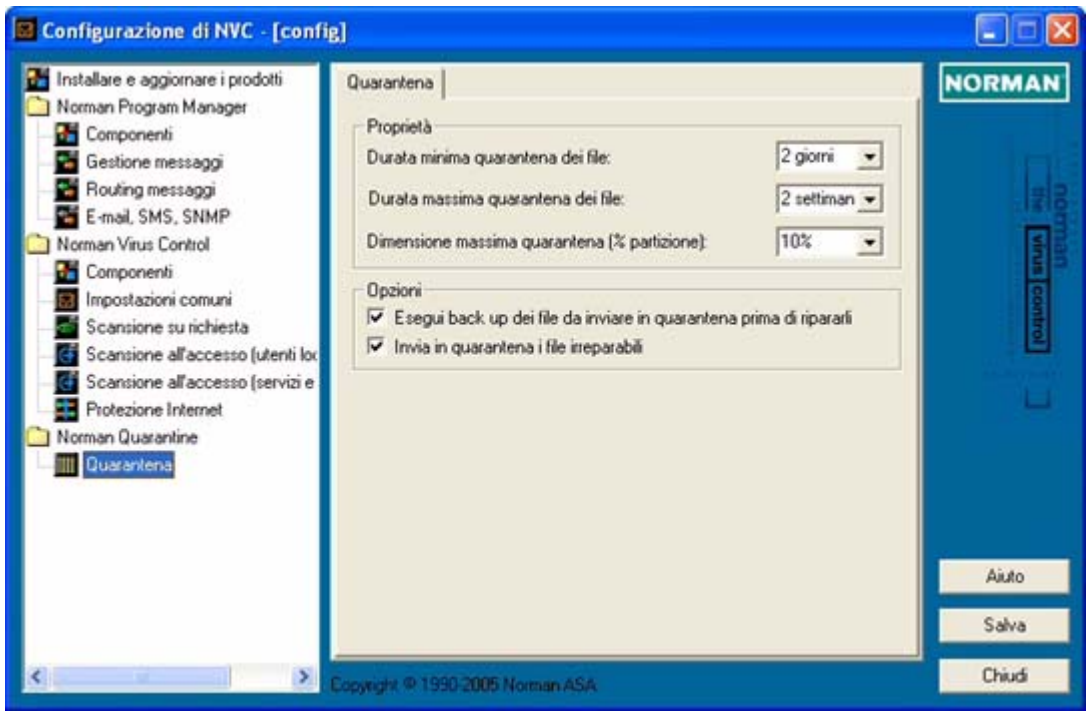
• **POP** (porta 110) è l'abbreviazione di *Post Office Protocol*

• **NNTP** (porta 119) è l'abbreviazione di *Network News Transfer Protocol*

Copyright © 1990-2005 Norman

Norman Quarantine

Quarantena



All'interno di questa scheda è possibile scegliere come gestire i file identificati da NVC come infetti o sospetti per altre ragioni. Se non si desidera ripulire o eliminare tali file, si consiglia di isolarli in un'area designata allo scopo, la quarantena.

Poiché all'installazione esistente sono stati aggiunti altri prodotti Norman, tali prodotti condividono questa funzione di quarantena e utilizzano le stesse opzioni specificate qui. Ciò consente di mantenere una strategia di quarantena uniforme.

Copyright © 1990-2005 Norman

Proprietà

Durata minima quarantena dei file:

Specificare un intervallo di tempo compreso tra un giorno e una settimana. I file con durata inferiore a quella minima specificata non vengono mai eliminati.

Durata massima quarantena dei file:

Specificare un intervallo di tempo compreso tra una e quattro settimane. I file che superano il periodo massimo specificato verranno eliminati senza preavviso.

Dimensione massima quarantena (% partizione):

Specificare la quantità di spazio disco dell'attuale partizione da riservare ai file in quarantena. La dimensione massima consentita può essere superata nel caso in cui i file in quarantena non abbiano ancora raggiunto la ***durata minima*** specificata.

Options

☑ Esegui back up dei file da inviare in quarantena prima di ripararli

Prima che NVC ripari un file infetto, è possibile eseguirne il back up. In linea generale, la riparazione di un file non comporta grossi rischi.

☑ Sposta in quarantena i file irreparabili

Nel caso in cui NVC non sia in grado di riparare un file, è possibile inviarlo nell'area destinata alla quarantena.

Indipendentemente dalla scelta effettuata dall'utente, NVC può comunque procedere, per motivi di sicurezza, alo spostamento dei file irreparabili in quarantena.

Nota: Indipendentemente dalla scelta effettuata dall'utente, NVC mette in quarantena i file che non possono essere riparati se nel modulo Scansione all'accesso (servizi e utenti remoti) è stata selezionata l'opzione **Analizza file nuovi o modificati** (pagina 63). La strategia impiegata per la scansione di file nuovi o modificati presuppone infatti un ambiente privo di virus. Di conseguenza, se la riparazione fallisce, al file infetto viene impedito di risiedere sulla macchina.

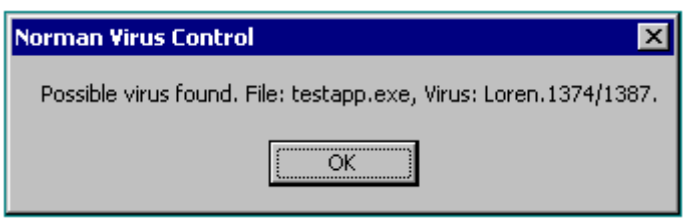
Copyright © 1990-2005 Norman

NVC sui Terminal Server di Windows

Nelle piattaforme Windows NT o Windows 2000 con Servizi terminal gli utenti si possono collegare al server tramite i client di Servizi terminal. Con questa configurazione i client di Servizi terminal non eseguono localmente le applicazioni, ma dipendono invece dal server per eseguire le istanze delle applicazioni che utilizzano. Il server distribuisce il layout della schermata ad ogni utente che si collega ed esegue le applicazioni per conto dell'utente.

Questa struttura semplifica all'amministratore la gestione dei file e delle applicazioni in un ambiente con più utenti. NVC ottimizza ulteriormente questa configurazione, in quanto risulta ancora più semplice da configurare per l'amministratore.

Durante la scansione all'accesso per le sessioni dei client di Terminal Server, NVC utilizza sempre la configurazione "servizi e utenti remoti" (oppure server). Ciò significa che non visualizza sul Terminal Server delle finestre di dialogo di avvertimento quando trova un virus. Sulla macchina del client di Terminal Server viene comunque visualizza una finestra di messaggio come questa:



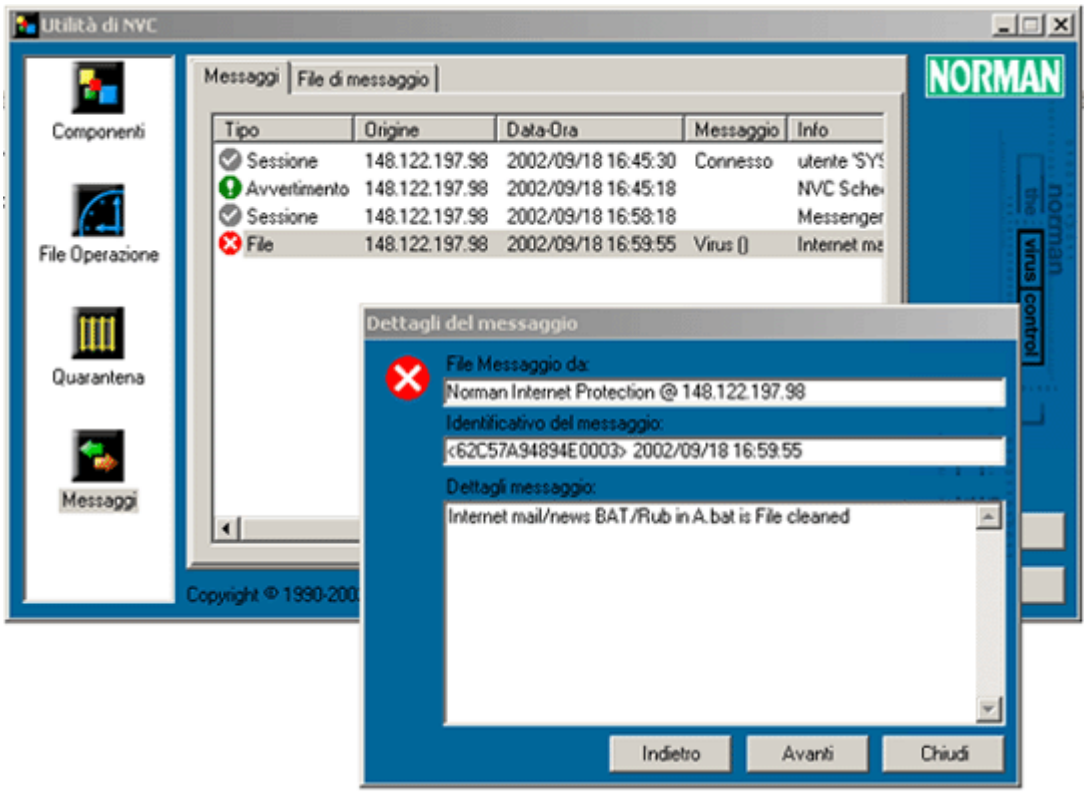
Questo messaggio è puramente informativo. Il client di Terminal Server non può cambiare le modalità o la configurazione della scansione.

L'impostazione predefinita della configurazione "servizi e utenti remoti" prevede solo la scansione dei file modificati o nuovi. I

Copyright © 1990-2005 Norman

file letti o eseguiti da un client di Terminal Server non vengono pertanto analizzati dalla scansione all'accesso.

Sulla Console messaggi di NVC dell'amministratore viene aggiunto il seguente messaggio:



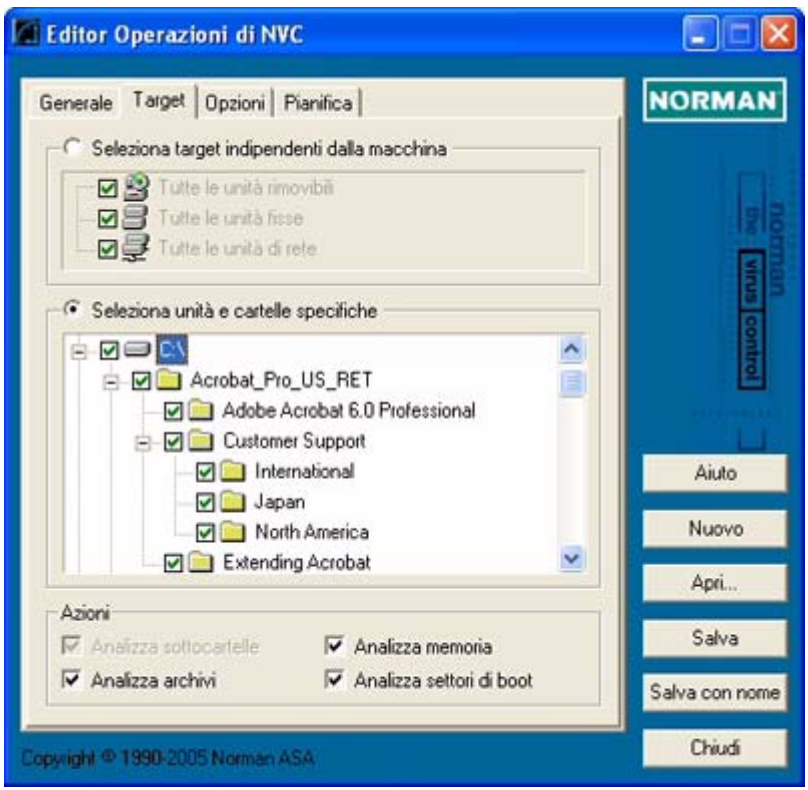
Al messaggio di avvertimento per virus viene aggiunto il nome del client di Terminal Server a cui ci si è connessi e della macchina del client di Terminal Server. Nell'esempio sopra illustrato l'utente PetterN sulla macchina NT2000PRO-BLI ha generato il messaggio di avvertimento per virus sul server terminal W2KTSRV.

È comunque possibile eseguire la scansione su richiesta di NVC da ogni sessione del Terminal Server. Questa funzione è identica alla scansione su richiesta eseguita su qualsiasi altra configurazione.

Copyright © 1990-2005 Norman

Editor Operazioni

A volte è pratico definire delle operazioni che devono essere eseguite più volte e/o a intervalli regolari. La ricerca di virus è un buon esempio di un'operazione che deve essere eseguita regolarmente, e l'Editor Operazioni è lo strumento fornito da NVC a questo scopo.



È possibile creare un file Operazione per le scansioni che si desidera eseguire regolarmente o per le scansioni speciali da eseguire in certe situazioni. Ad esempio, se si scaricano dei file da Internet in determinate aree, è possibile creare un file Operazione che analizza solo queste aree ed esegue l'operazione manualmente dopo il download. Inoltre è possibile pianificare l'esecuzione dell'operazione in un orario predefinito.

Copyright © 1990-2005 Norman

Gli amministratori possono creare dei file Operazione e distribuirli a tutte le workstation in rete per garantire che le aree che richiedono un'attenzione particolare vengano controllate regolarmente.

La posizione di default in cui vengono memorizzati i file Operazione è `...\nvc\tasks`. È possibile visualizzarli, modificarli, eseguirli ed eliminarli da Utilità di NVC (vedere pagina 98).

Nelle sezioni seguenti sono descritte le quattro schede dell'**Editor Operazioni**.

Generale

Nella scheda **Generale** utilizzare la casella **Descrizione** per immettere una breve descrizione dell'operazione. Se si creano più operazioni, può essere utile in un secondo tempo vedere perché era stata creata una determinata operazione in un certo momento, ad esempio potrebbe dipendere da un evento particolare.

Da **Utilità**|**File Operazione** è possibile visualizzare l'elenco completo dei file Operazione esistenti.

⇨ ‘Utilità' a pagina 98.

Target

In questa scheda è possibile specificare quali aree si desidera analizzare e come eseguire la scansione e salvare le opzioni scelte in un file Operazione.

Questa scheda è suddivisa in due sezioni: la prima per entità di grandi dimensioni, ad esempio le unità disco, la seconda per target di scansione più specifici.

All'interno di un file Operazione non è possibile combinare un'opzione della prima sezione con una della seconda. Ad esempio, non è possibile selezionare tutte le unità rimovibili e una cartella specifica di un'unità fissa.

Copyright © 1990-2005 Norman

Selezione dei target

Per entrambe le sezioni di questa scheda la procedura da seguire per includere le aree da sottoporre a scansione e salvare le opzioni scelte in un file Operazione è la seguente:

1. Fare clic sul pulsante di opzione ⊙ per attivare la sezione desiderata.
2. Fare clic sulle aree che si desidera includere nella scansione. È possibile aggiungere più aree da analizzare in ogni sezione.
3. Se si selezionano unità e cartelle specifiche, vengono selezionate automaticamente tutte le sottocartelle dell'unità/cartella selezionata. È possibile deselezionare le sottocartelle che non si desidera includere nella scansione.
4. Al termina, fare clic su **Salva** per memorizzare le selezioni in un file Operazione. La posizione di default in cui viene memorizzato il file Operazione è `...\nvc\tasks`.

Nota: Se si pianifica un file Operazione, **deve** trovarsi nella directory `...\nvc\tasks`.

5. Per modificare un file Operazione esistente, fare clic su **Apri** e selezionare il file dalla finestra di dialogo Apri. Apportare le modifiche desiderate e fare clic su **Salva**.

Seleziona target indipendenti dalla macchina

In un file Operazione è possibile scegliere una, due o tutte le opzioni.

Copyright © 1990-2005 Norman

☑ **Tutte le unità rimovibili**

Seleziona tutte le unità floppy, le unità CD-ROM e altre unità rimovibili disponibili nel sistema.

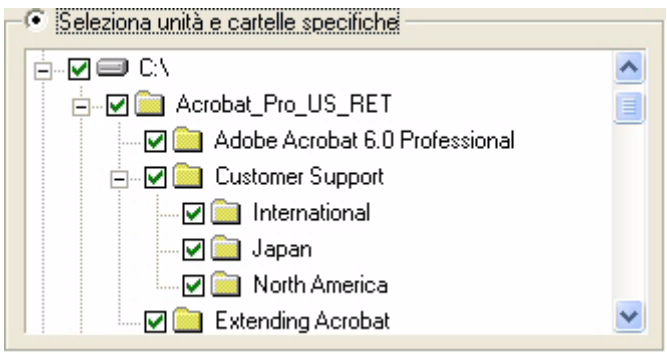
☑ **Tutte le unità fisse**

Seleziona tutte le unità fisse locali del sistema.

☑ **Tutte le unità di rete**

Seleziona tutte le unità di rete riconosciute dal sistema.

Seleziona unità e cartelle specifiche



Quando, ad esempio, si seleziona un'unità, tutte le cartelle e le sottocartelle di tale unità vengono selezionate automaticamente per la scansione. Allo stesso modo, se si seleziona una cartella o una sottocartella, vengono incluse tutte le cartelle in essa contenute. Per escludere dalla scansione una sottocartella, fare clic su di essa per deselezionarla.

Opzioni di scansione comuni

Nella parte inferiore della pagina vi è un gruppo di opzioni di scansione comuni sotto *Azioni*:

☑ **Analizza sottocartelle**

Se si sono selezionate una o più unità o directory, questa opzione consente di includere nella scansione anche le sottodirectory.

Copyright © 1990-2005 Norman

☑ **Analizza archivi**

Selezionare questa opzione per includere nella scansione i file d'archivio. Attualmente sono supportati i seguenti formati: ZIP, ARJ, RAR, ACE, ARC, GZIP, TAR e BZIP2.

☑ **Analizza memoria**

Quando si analizza l'area della memoria, NVC cerca i virus residenti. Controllare sempre che non vi siano virus nella memoria.

☑ **Analizza settori di boot**

Quando si seleziona questa opzione, NVC controlla il settore di boot dell'area analizzata.

Opzioni

Utilizzare questa scheda per decidere il livello di visibilità di NVC durante una scansione e quante risorse di sistema assegnare a NVC.

Finestra di scansione:

Autostart: Nascosta, visualizza solo se la pulizia fallisce

Con questa opzione NVC viene eseguito in modalità invisibile e viene visualizzato solo se rileva un virus che non riesce a eliminare. Dato che è complicato annullare un'operazione eseguita in modalità nascosta, questa opzione può risultare utile per gli amministratori che desiderano che le operazioni vengano eseguite in base alla pianificazione e per scoraggiare i singoli utenti che potrebbero incontrare difficoltà nell'annullamento di una scansione in corso. Se questa opzione è selezionata, un'operazione pianificata viene avviata automaticamente.

Autostart: Minimizzata, visualizza solo se la pulizia fallisce

Con questa opzione NVC viene eseguito in una finestra ridotta a icona e viene visualizzato solo se rileva un virus che non riesce a eliminare. Se questa opzione è selezionata, un'operazione pianificata viene avviata automaticamente.

Copyright © 1990-2005 Norman

⊙ **Autostart: Minimizzata, visualizza solo se è rilevata l'infezione**

Con questa opzione NVC viene eseguito in una finestra ridotta a icona e viene visualizzato solo in presenza di un virus. Se questa opzione è selezionata, un'operazione pianificata viene avviata automaticamente.

O **Avvio manuale: Finestra normale**

Con questa opzione NVC viene eseguito in una finestra aperta durante la scansione. Quando si pianifica una scansione con questa opzione attivata, all'orario pianificato viene visualizzata la finestra di dialogo della scansione ed è necessario avviarla ***manualmente*** facendo clic su **Analizza.**

Utilizzo risorse:

In condizioni di funzionamento normali, è difficile che un computer esaurisca le risorse interne al punto tale che il sistema operativo è costretto a definire un elenco di priorità per le operazioni da eseguire. Se si dovesse verificare questa situazione, se si seleziona **Basso** NVC aspetta che si liberino le risorse del sistema prima di eseguire la scansione, mente se si seleziona **Normale** NVC si troverà insieme alle altre operazioni in attesa di essere eseguite.

Basso e **Normale** hanno un effetto diverso a seconda del sistema operativo in esecuzione.

Programma

Una volta impostato un file Operazione utilizzando le schede illustrate in questo capitolo, è possibile pianificare l'esecuzione di scansioni ripetitive sul computer.

☑ **Operazione pianificata**

Se si desidera utilizzare il pianificatore, accertarsi che questa opzione sia selezionata. Per eseguire un'operazione pianificata è necessario: 1) che sia contrassegnata l'opzione **Operazione pianificata** e che 2) il file Operazione sia residente nella directory `...\nvc\tasks`.

Copyright © 1990-2005 Norman

Frequenza

Poi si deve decidere quando eseguire l'operazione ed è possibile scegliere tra diversi intervalli, da **Una volta** a **Ogni mese**.

Data/ora di inizio:

Specificare il giorno/mese/anno in cui si desidera eseguire per la prima volta l'operazione pianificata. Per modificare la data, utilizzare i tasti freccia della tastiera (oppure fare clic sulle frecce nella casella). È possibile evidenziare la data, il mese e l'anno e modificare i valori utilizzando la tastiera. Il giorno della settimana cambia automaticamente a seconda della data selezionata.

☐ **Coordinate Tempo Universale (UTC)**

Questa opzione risulta particolarmente utile per le aziende che hanno sedi in tutto il mondo e desiderano eseguire simultaneamente le scansioni indipendentemente dall'ora locale.

Informazioni sul pianificatore

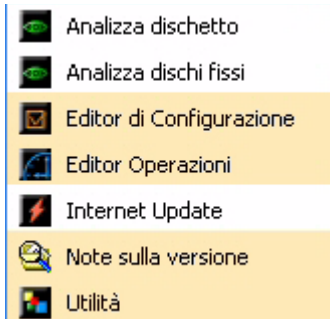
L'obiettivo principale del pianificatore è eseguire i file Operazione nell'orario specificato. È possibile pianificare che un file Operazione venga eseguito ogni giorno, una volta alla settimana, una volta al mese oppure solo una volta. È necessario immettere la data e l'ora di inizio e i valori di default sono la data e l'ora corrente.

Per le aziende che hanno sedi con fusi orari diversi, la funzione Coordinate Tempo Universale (UTC) consente di eseguire un'operazione simultaneamente indipendentemente dal fuso orario.

Il pianificatore cerca sempre nella sottodirectory "Operazioni" i processi pianificati e pertanto è necessario tenere la struttura `...\nvc\tasks` per eseguire un'operazione pianificata.

Copyright © 1990-2005 Norman

Utilità



Le utilità di NVC sono uno strumento che fornisce una panoramica dello stato corrente dei componenti di NVC sul PC. Oltre a visualizzare le informazioni chiave, è possibile modificare alcuni elementi selezionando alcune voci, ad esempio i file Operazione.

È possibile accedere al modulo Utilità dal menu Norman sotto la 'N' nella barra delle applicazioni oppure dal percorso Start|Programmi|Norman Virus Control.

In questa versione il gruppo Utilità è composto da tre categorie principali:

- File Operazione
- Quarantena
- Messaggi

File Operazione

Quando si crea un file Operazione con l'Editor Operazioni di NVC, il file viene salvato per default in `...\nvc\tasks`.

Nota: Per poter pianificare un'operazione, il file Operazione deve trovarsi in questa directory.

Per visualizzare questa director è possibile utilizzare, ad esempio, Esplora risorse o l'Editor Operazioni. Tuttavia lo strumento più flessibile è questa finestra di dialogo, che consente di visualizzare, modificare, creare e aprire i file Operazione in modi diversi. Inoltre in essa è visualizzato lo stato di tutti i file Operazione.

È possibile seguire i file Operazione dalla linea di comando. Questo processo richiede l'avvio della scansione su richiesta e l'esecuzione di un'operazione specifica dalla riga di comando nascosta all'utente.

⇨ Vedere ‘Esecuzione dei file Operazione dalla linea di comando' a pagina 111.

Copyright © 1990-2005 Norman

Campi presenti nella finestra di dialogo File Operazione

File Operazione

Mostra il nome del file Operazione.

Pianificazione

Mostra l'eventuale pianificazione del file Operazione e i relativi intervalli specificati.

Prossimo avvio

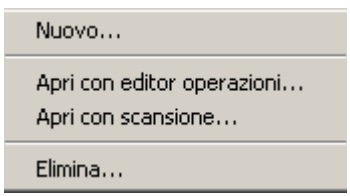
Mostra giorno, mese e ora della prossima esecuzione del file Operazione. Se l'operazione non è stata pianificata, questo campo risulterà vuoto.

Ultimo avvio

Mostra l'ultima volta in cui il file Operazione è stato eseguito con successo. Se l'operazione non è stata pianificata, questo campo risulterà vuoto.

Opzioni del Menu di scelta rapida

È possibile evidenziare una voce alla volta e, premendo il pulsante destro del mouse, selezionare le opzioni dal seguente menu:



Nuovo

Apre l'Editor Operazioni, consentendo la creazione di un nuovo file Operazione.

Apri con editor Operazioni

Apre il file Operazione nell'Editor Operazioni per consentirne la modifica.

Apri con scansione

Apre il file Operazione per la scansione, consentendone l'esecuzione immediata.

Copyright © 1990-2005 Norman

Cancella

Elimina il file selezionato.

Quarantena

Se sono state attivate le opzioni di quarantena nel modulo Impostazioni comuni (‘Quarantena' a pagina 87), in questa finestra di dialogo vengono visualizzati i file idonei per la quarantena. Questi file sono infetti, hanno un formato sconosciuto o sono bloccati da Norman Internet Protection (NIP). Consultare la sezione ‘Blocco degli allegati' a pagina 81.

Campi presenti nella finestra Quarantena:

File in quarantena

Mostra il percorso (se applicabile) e il nome del file in quarantena. In alcune situazioni non è possibile visualizzare il percorso, ad esempio per gli allegati di posta elettronica che vengono sempre controllati in un'area temporanea del disco.

Data

Mostra la data in cui il file è stato posto in quarantena.

Dimensione

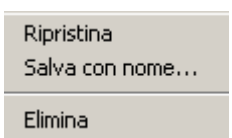
Mostra la dimensione del file posto in quarantena.

Diagnosi

Mostra lo stato del file. Le diagnosi possibili sono: Infetto, Sconosciuto.

Opzioni del Menu di scelta rapida

È possibile evidenziare una voce alla volta e, premendo il pulsante destro del mouse, selezionare le opzioni dal seguente menu:



Copyright © 1990-2005 Norman

Ripristina

Riporta il file alla sua forma originaria nella cartella originaria. Per gli allegati di posta elettronica viene visualizzato solo un nome file ed è necessario utilizzare l'opzione **Salva con nome**.

Salva con nome

Permette di scegliere il nome del file e la posizione in cui salvarlo.

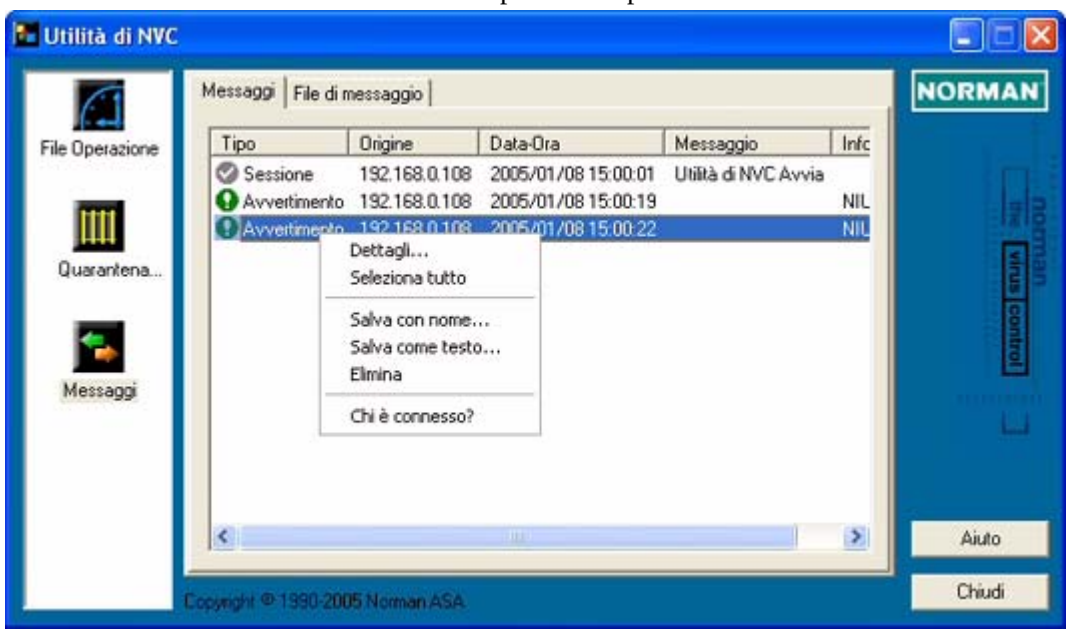
Cancella

Elimina completamente il file.

Messaggi

Scheda Messaggi

Se è stato attivato il servizio messaggi (vedere ‘Logger messaggi' a pagina 35), i tipi di messaggio selezionati possono essere visualizzati e modificati in questa scheda. Selezionare una voce dall'elenco e premere il pulsante destro del mouse:



Copyright © 1990-2005 Norman

Campi presenti nella scheda Messaggi

Tipo

Fornisce informazioni su tipo e categoria del messaggio accanto ad una icona che ne indica tipo e gravità. Le voci visualizzate corrispondono ai tipi di messaggio specificati nel Logger dei messaggi.

Origine

Indica l'indirizzo IP della macchina che ha generato il messaggio.

Data-Ora

Mostra anno/mese/giorno e ora/minuti/secondi in cui ha avuto luogo l'evento che ha dato origine al messaggio.

Messaggio

Mostra una parola chiave relativa all'evento, come ad esempio: "Virus", "Connesso", ecc.

Info

Consiste in una riga di testo descrittiva del messaggio.

Opzioni del Menu di scelta rapida:

Dettagli

Visualizza una finestra di dialogo che fornisce informazioni sull'origine e l'identificativo del messaggio e mostra una casella di testo contenente ulteriori dettagli.

Seleziona tutto

Permette di selezionare tutti i messaggio/voci per eseguire su di essi eventuali operazioni di salvataggio, visualizzazione dettagli, eliminazione ecc.

Salva con nome

Permette di salvare uno o più messaggi con il nome desiderato. Per accedere ai messaggi salvati in qualsiasi momento è sufficiente spostarsi nella scheda successiva **File di messaggio**. I messaggi vengono salvati con estensione `.nps`.

Salva come testo

Salva le voci selezionate in un file di testo con il nome desiderato

Copyright © 1990-2005 Norman

Cancella

Consente di eliminare un messaggio.

Chi è connesso?

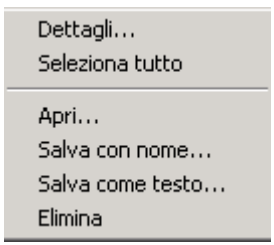
Consente di trasmettere il messaggio.

Scheda File di messaggio

Se uno o più messaggi sono stati salvati come file con la funzione **Salva con nome** della scheda **Messaggi**, è necessario aprirli nella scheda **File di messaggio** .

I campi sono identici a quelli presenti nella **scheda Messaggi**.

Opzioni del Menu di scelta rapida



Le opzioni attivabili tramite il pulsante destro del mouse sono le stesse descritte a proposito della **scheda Messaggi** fatta eccezione per:

Apri

Posizionare il cursore nella casella di testo vuota, premere il pulsante destro del mouse e selezionare **Apri** per poter visualizzare la relativa finestra di dialogo. Vi si troveranno elencati tutti i file salvati (con estensione `.nps`) nella directory di default `...\norman\msg`.

Copyright © 1990-2005 Norman

Aggiornamento di NVC

La versione più aggiornata di un antivirus è anche quella più efficace e quindi è fondamentale aggiornarlo di frequente per proteggere il proprio ambiente di lavoro.

A coloro che non si servono di Norman Program Manager (NPM) per distribuire gli aggiornamenti di NVC in una rete locale, si consiglia di utilizzare in alternativa Norman Internet Update o semplicemente Internet Update (IU). Internet Update è un programma che assicura l'esecuzione della versione corrente di NVC per la piattaforma in uso controllando nei server Norman la disponibilità di eventuali modifiche a NVC, quali modifiche al programma, correzioni di errori, un nuovo motore di scansione e file di definizione aggiornati. Quando si esegue IU, il programma confronta i componenti di NVC installati sul computer con la versione corrispondente presente sul server dei prodotti Norman. Se la data e l'ora sono diversi, è possibile scaricare gli aggiornamenti. In teoria potrebbe essere stato modificato tutto il programma e di conseguenza potrebbe essere necessario scaricarlo tutto.

Internet Update viene visualizzato separatamente nel gruppo di programmi Norman.

Per eseguire IU, è necessaria una connessione TCP/IP (Internet).

Gli utenti singoli possono utilizzare IU per scaricare direttamente sulla loro macchina locale gli aggiornamenti mentre gli amministratori possono scaricare gli aggiornamenti su un server per far poi distribuire da NPM i pacchetti aggiornati alle workstation in rete.

Norman Internet Update

Avvio di Internet Update

Per avviare Internet Update, scegliere Start|Programmi|Norman Virus Control|Internet Update oppure selezionare ***Internet Update*** dal menu visualizzato quando si fa clic sull'icona

Copyright © 1990-2005 Norman

Norman nella barra delle applicazioni (nell'angolo in basso a destra dello schermo).

OS/2 WARP

Fare clic con il pulsante destro del mouse sul desktop e selezionare *Norman Virus Control*.

Internet Update e connessione Internet

Per eseguire Internet Update (IU), è necessaria una connessione TCP/IP (Internet).

Nell'Editor di Configurazione, specificare in che modo si desidera eseguire l'aggiornamento tramite Internet, come descritto a pagina 26. Se si seleziona **Tramite connessione diretta a orario programmato** e si fa clic sul pulsante **Impostazioni**, è possibile immettere l'intervallo quando si esegue la ricerca degli aggiornamenti:

L'opzione **Solo su richiesta (avvia manualmente)** si basa interamente sull'azione manuale dell'utente, che deve ricordarsi autonomamente di avviare Internet Update nel momento desiderato, salvo nel caso in cui i file di definizione non siano stati aggiornati da più di due mesi.

Con l'opzione **Ogni giorno tramite connessione via modem (attendi connessione)** IU controlla una volta al giorno se ci sono aggiornamenti. Il controllo avviene se si ha una connessione a Internet via modem.

Nel caso di connessione diretta a Internet (linea commutata o modem via cavo), è possibile scegliere **Tramite connessione diretta a orario programmato**. In questo modo è possibile programmare quando eseguire IU ed integrare eventualmente gli

Copyright © 1990-2005 Norman

aggiornamenti di NVC nelle altre operazioni pianificate. Vedere la parte superiore della pagina.

In altre parole, le ultime due opzioni consentono di aggiornare automaticamente NVC tramite Norman Internet Update.

Nota: Se la macchina dove si stanno scaricando gli aggiornamenti è protetta da un firewall, potrebbe essere necessario immettere l'indirizzo e la porta del proxy HTTP del firewall. Fare riferimento alle impostazioni del server proxy a pagina 30.

Funzionamento di Internet Update

Ad eccezione dell'opzione **Su richiesta** che si basa su un input manuale, IU si avvia in "modalità nascosta", ovvero l'utente non vede nulla fino a quando IU ha stabilito se vi sono aggiornamenti disponibili. Se non ve ne sono, IU si disattiva.

In questa fase iniziale IU invia al server Norman la chiave di convalida per verificare la licenza e una "stringa di profilo". La stringa di profilo contiene delle informazioni quali la versione del sistema operativo e della lingua della macchina, elementi che determinano quali sono gli aggiornamenti idonei per quella macchina.

Per gli amministratori:

IU gestisce anche le reti con workstation che eseguono sistemi operativi diversi. Quando l'amministratore esegue il programma `niucf.exe` (memorizzato nella cartella `...\nvc\bin`), viene creato un file `niucf.ndf` nella cartella `...\nvc\config`. Questo file è un modulo d'ordine in cui sono memorizzate tutte le informazioni necessarie relative alla piattaforma, alla lingua e ai prodotti. IU controlla che il contenuto del file appaia nell'elenco degli aggiornamenti idonei, a condizione che la licenza copra gli articoli ordinati. È necessario eseguire `NIUcf` prima di eseguire Internet Update la prima volta.

Le attività di IU si possono suddividere in tre fasi distinte:

Fase 1:

Invia la chiave di convalida e la stringa del profilo a un server di convalida Norman. Il server restituisce un elenco di pacchetti. I

Copyright © 1990-2005 Norman

pacchetti contengono il codice del programma NVC, i file di definizione dei virus o altre funzioni di NVC.

Fase 2:

IU confronta la data e l'ora di un pacchetto sul server dei prodotti con la data e l'ora del pacchetto presente nella directory locale di download. È possibile effettuare il download di un pacchetto sul server dei prodotti Norman se la data e l'ora del pacchetto locale è diversa oppure se manca il pacchetto.

Se sono disponibili dei nuovi pacchetti, viene visualizzata una finestra di dialogo che specifica la dimensione totale dei pacchetti. La finestra di dialogo ha una funzione timer e, se non si seleziona **Sì/No** entro 15 secondi, inizia il download.

Fase 3:

In questa fase vengono scaricati i nuovi pacchetti nella directory di download.

Una volta completato il download, IU si disattiva e si attiva Norman Program Manager (NPM) che aggiorna NVC sulla macchina.

LAN/WAN

In un ambiente di rete è possibile aggiornare le workstation selezionando **Automaticamente dal server**.

Si noti che l'opzione di aggiornamento dal server utilizza le informazioni immesse nella finestra di dialogo con schede **LAN/WAN**.

Copyright © 1990-2005 Norman

Informazioni varie su NVC

Norman Program Manager (NPM)

NPM richiede una spiegazione più dettagliata rispetto agli altri prodotti, anche in quanto risulta fondamentale per NVC e per gli altri programmi Norman. NPM partecipa all'installazione, all'aggiornamento e alla comunicazione con altri programmi e moduli, ed è raramente visibile all'utente anche se sempre in esecuzione.

Il nome file principale di NPM è `Zanda.exe`, che è l'abbreviazione di Zero Administration Network Distribution Agent. NPM è il collegamento tra i componenti che devono comunicare tra loro ed è pertanto fondamentale per NVC. Come suggerisce il nome, è più occupato in una rete che in un computer autonomo e pertanto è illustrato più dettagliatamente nel *Manuale dell'amministratore*.

Norman Program Manager risiede *localmente*, ovvero sulla workstation o sul server. NPM recupera i file dal server su richiesta della workstation. Ad esempio, se il file della configurazione specifica che la workstation deve scaricare gli aggiornamenti dal server ogni giorno, NPM provvede al *recupero* dei file. Inoltre l'agente *invia* i messaggi dalla workstation al server. Si noti che la collaborazione tra Norman Program Manager e IU è particolarmente importante durante gli aggiornamenti: un aggiornamento *non* è completo fino a quando NPM non ha decompresso e installato i nuovi file.

Norman Program Manager è sempre in esecuzione.

Le operazioni di competenza di NPM sono:

- Gestione degli aggiornamenti di NVC
- Controlla che i moduli si siano avviati come impostato nella configurazione.
- Controllo della conformità della configurazione in base ai requisiti dell'amministratore per la singola workstation

Copyright © 1990-2005 Norman

- Download degli aggiornamenti del software, della nuova configurazione e dei file Operazione

⇨ ‘LAN/WAN' a pagina 21.

- È dotato di un proprio pianificatore.

Per informazioni più dettagliate sull'agente consultare il*Manuale dell'amministratore*.

Informazioni sulla scansione da linea di comando

Oltre alla Scansione su richiesta e alla Scansione all'accesso disponibili nell'interfaccia utente, NVC offre una versione della scansione dalla linea di comando

La scansione da linea di comando di NVC ha le stesse funzioni di base delle scansioni da menu.

Questo tipo di scansione non dipende da nessun altro modulo e si può eseguire dai file batch.

Avvio della scansione da riga di comando

1. Dal prompt di DOS o OS/2 andare nella directory in cui risiede NVC.
2. La sintassi è:

   ```
   nvcc [unità]:[percorso] [/parametri]
   [Invio]
   ```

   Ogni parametro utilizzato deve essere preceduto da uno spazio.

   Selezionare semplicemente la combinazione di parametri che si desidera utilizzare e specificarli nella linea di comando.

⇨ Per una panoramica completa e una spiegazione dei parametri disponibili consultare ‘Opzioni della scansione da linea di comando' a pagina 111.

Copyright © 1990-2005 Norman

Pulizia dei file infetti

Nota: Nel software e nella documentazione di NVC i termini "riparazione", "rimozione" e "pulizia" sono intercambiabili. Si riferiscono tutti alla procedura di rimozione dei virus dai file o dai settori di boot e al ripristino della condizione originale dell'area infetta.

Il cuore della tecnologia delle scansioni di NVC (scansione su richiesta, all'accesso e da linea di comando) è il motore di scansione. Le opzioni di scansione riflettono le capacità del motore. Oltre a rilevare i virus, il motore è anche in grado di rimuoverli (***riparare*** il file o il settore di boot e di conseguenza ***pulire*** la macchina). Questo processo è tecnicamente più complicato del rilevamento dei virus.

Se tutto il file è costituito da codice dannoso, come nel caso dei **cavalli di troia**, non c'è nulla di riparabile. In questi casi, l'unico intervento possibile è l'*eliminazione* dell'intero file. Per questo motivo a volte si utilizza l'espressione "pulizia con eliminazione".

Con le scansioni è possibile rimuovere automaticamente tutti i tipi di virus dalle unità fisse e dai floppy, ad eccezione dei ***virus del settore di boot***. È possibile farlo automaticamente dai floppy, ma non dalle unità fisse.

Se non si verificano inconvenienti, riparare un file è meno complicato che riparare un settore di boot. Un settore di boot danneggiato può rendere inutilizzabile il sistema. Per garantire che la riparazione di un settore di boot danneggiato non abbia delle ripercussioni spiacevoli per l'utente, NVC non consente di riparare automaticamente i settori di boot delle unità fisse.

Se NVC rileva un virus del settore di boot, viene visualizzata una finestra di dialogo che consiglia di eseguire una copia di riserva su floppy di tutti i dati necessari. Se la riparazione fallisce, è possibile avviare la macchina dal floppy di ripristino. Una finestra di dialogo completa di Guida di linea guida l'utente nel caso in cui venga rilevato un virus del settore di boot.

Copyright © 1990-2005 Norman

Esecuzione dei file Operazione dalla linea di comando

È possibile avviare NVCOD dalla linea di comando per eseguire un file Operazione da questo ambiente.

NVCOD può utilizzare un file Operazione esistente, se si immette il comando seguente:

`NVCOD @<percorso del file Operazione>`

Questa funzione è utile in quanto l'operazione viene eseguita in modalità nascosta per l'utente, ad esempio può servire come metodo di scansione degli script di login.

Esempio:

Si supponga di aver creato un'operazione denominata `scansione.sdf`. Il file si trova nella libreria predefinita `c:\norman\nvc\tasks`. Si desidera analizzare la macchina con le opzioni specificate nel file Operazioni invece che analizzare tutto il disco fisso utilizzando l'opzione**Analizza dischi fissi**.

Dalla linea di comando immettere:

```
c:\norman\nvc\bin>nvcod.exe
@c:\norman\nvc\tasks\miascansione.sdf
```

Opzioni della scansione da linea di comando

Dalla directory in cui risiede il programma Norman eseguire il comando

`nvcc /?`

dalla linea di comando per visualizzare l'elenco delle opzioni disponibili. Le tabelle seguenti illustrano i parametri disponibili e le relative funzioni.

Copyright © 1990-2005 Norman

Param.:	Funzione:
/-help	Mostra la guida in linea.
/?	Mostra la guida in linea.
/ALD	Analizza tutti i dischi locali (non i floppy o i CD-ROM)
/AD	Analizza tutti i dischi (non i floppy). Oltre alle unità fisse locali vengono analizzate tutte le unità di rete.
/B	Non emette un segnale acustico quando rileva delle infezioni (DISATTIVATO di default).
/BS-	Non analizza le area di sistema. Le aree di sistema della stessa unità vengono analizzate solo una volta se vengono specificate per la stessa unità logica più specifiche di file (DISATTIVATO di default).
/BS+	Analizza solo le aree di sistema.
/C:	Analizza i file d'archivio. /C:0 no, /C:1 sì (impostazione predefinita in config).
/C	Analizza i file d'archivio. Uguale a /C:1 (impostazione predefinita in config).
/CP	Analizza i file di programma compressi (DISATTIVATO di default)
/CL:	Ripara i file e i settori di boot: /CL:0 no, /CL:1 sì, /CL:2 anche all'interno di archivi (impostazione predefinita in config).
/CL	Ripara i file e i settori di boot. Uguale a /CL:1 (default in Config).
/CZ:	Dimensione massima di file d'archivio in KB. Implica /C (default in Config).
/CR:	Profondità ricorsiva massima dei file d'archivio. Implica /C (default in Config).
/FLOPPY	Legge i file NSE da un floppy separato (solo DOS)

Copyright © 1990-2005 Norman

Param.:	Funzione:
/H	Mostra la guida in linea.
/HUM	Gestisce le macro non certificate (occorre NSE\NVCMACRO.CRT di CatsClaw).
/L:	Imposta il livello di log: /L:0=no, 1=sì, 2=dettagliato (impostazione predefinita in config).
/LD:	Specifica la directory dei file di log (directory predefinita in Config).
/LF:	Specifica il nome completo del file di log (ignora LD: e /LG:). Digitare il nome subito dopo il parametro (senza spazi).
/LG:	Specifica il numero di generazioni del file di log (numero predefinito in Config).
/N	Sopprime l'analisi di default della memoria.
/O	Ignora i file bloccati (DISATTIVATO di default).
/Q	Modalità quiete, ovvero nessun output su schermo (DISATTIVATO di default).
/R	Ripete la scansione. Utile per controllare più floppy (DISATTIVATO di default).
/S	Analizza le sottodirectory. Utilizzare questa opzione se è stata specificata una directory e si desidera includere nella scansione le sottodirectory. Se è stata specificata la lettera di un'unità, le sottodirectory vengono incluse automaticamente nella scansione. Impostazione di default per la scansione delle unità.
/SB	Utilizza Sandbox. 0=Disattivato, 1=Attivato
/SN	Non consente agli utenti di interrompere l'esecuzione (DISATTIVATO di default).

Copyright © 1990-2005 Norman

Param.:	Funzione:
/TEMP:	Ignora gli ambienti TEMP/TMP. Se non è stato definito un ambiente di questo tipo, il programma lo crea di un livello superiore rispetto alla posizione della directory NSE.
/U	Non si interrompe quando rileva delle infezioni (DISATTIVATO di default).
/V	Modalità dettagliata (DISATTIVATO di default).
/W:	Attende il numero specificato di millisecondi tra ogni file (0 di default).
/YH	Si interrompe quando rileva un'infezione (DISATTIVATO di default).

Abbinamento dei diversi parametri

La scansione da linea di comando è flessibile in quanto consente di abbinare i parametri per eseguire più operazioni con un solo comando.

Qui di seguito sono riportati alcuni esempi di abbinamento dei parametri. Dalla directory in cui è installato `nvcc.exe` digitare:

```
nvcc c:\*.exe /s /u /cl /lf:myscan.log
```

per effettuare la scansione di tutti i file con estensione `.exe` sull'unità c: compreso le sottodirectory. La scansione non viene interrotta in caso di rilevamento di file infetti, i file potenzialmente infetti vengono puliti e viene creato il registro `scansione.log` nella directory in cui è installato `nvcc.exe` .

Quindi digitare:

```
nvcc *.txt a: c:
```

per analizzare i file `txt` nella directory corrente e poi le aree di boot e le estensioni dei file di default in `a:` e `c:`.

Nota: Se si digita `c:\` (con una barra), vengono analizzati solo i file presenti nell'unità principale, mentre se si digita `c:`

Copyright © 1990-2005 Norman

(senza barra), vengono analizzati sia i file sia le aree di sistema del disco.

Livelli di errore della scansione da linea di comando

È possibile automatizzare le scansioni da linea di comando utilizzando i livelli di errore in file batch. I livelli di errore delle scansioni da linea di comando sono::

Livello di errore:	**Significato:**
13	La licenza non consente l'avvio del programma.
12	Non è stato trovato il file `NVC32.CFG`.
11	Sono stati trovati alcuni file o archivi danneggiati.
10	Non è stato possibile aprire tutti i file per analizzarli.
9	Scansione interrotta dall’utente.
8	Errore interno: scansione interrotta.
7	Avvertimento. Impossibile trovare alcuni componenti come `Nlog5.dll`.
6	Errore di input/output del disco.
5	Errore di utilizzo: parametro non valido oppure argomento di parametro dato.
4	La configurazione dell'hardware è stata modificata dopo l'installazione del motore di scansione.
3	Errore di utilizzo: la scansione è cominciata prima di aver specificato dei criteri di scansione.
2	È stato trovato un virus attivo nella memoria ed è stato rimosso.

Copyright © 1990-2005 Norman

Livello di errore:	**Significato:**
1	Virus trovato e/o riparato. Questo codice di errore sostituisce tutti i codici di errore ad eccezione del 2.
0	Tutto OK. Non è stato trovato nessun virus o altro codice dannoso.

Copyright © 1990-2005 Norman

Appendice A - Sandbox

Premessa

L’idea di inventare un metodo che rileva nuovi virus sconosciuti è vecchia quanto il settore degli antivirus. Nel corso degli anni le aziende che sviluppano antivirus hanno investito notevoli risorse per giungere a una soluzione che potesse realizzare questo obiettivo ambizioso.

In occasione della Virus Bulletin Conference del 2001 Norman ha presentato un prototipo perfettamente funzionamento di un motore di scansione con funzionalità sicure (Sandbox).

Cos’è un “sandbox”?

Sandbox è il termine che meglio descrive la tecnica utilizzata per controllare se un file è stato infettato da un virus sconosciuto. Il nome non è stato scelto a caso perché questo metodo consente di far “giocare" del codice, probabilmente infetto e considerato non attendibile, non nel computer vero bensì in un’area simulata e limitata al suo interno. Il "sandbox” è dotato di tutto ciò che un virus si aspetta di trovare in un computer vero. In questa specie di parco giochi si consente al virus di replicarsi ma al tempo stesso si controlla e si registra ogni suo passo. Il virus si espone e dato che le sue azioni vengono registrate è possibile generare automaticamente un rimedio.

Oggi un worm di posta elettronica può infettare decine di migliaia di workstation in pochi secondi. Dai fornitori di antivirus ci si aspetta che trovino un rimedio, aggiornino i file di definizione dei virus e li distribuiscano immediatamente ai propri clienti. È fondamentale essere veloci perché la natura del codice dannoso di oggi è tale da paralizzare intere reti e causare gravi danni a un numero illimitato di computer.

Copyright © 1990-2005 Norman

Tecniche di sicurezza con Sandbox

Tecniche di sicurezza con Sandbox - emulazione

Un virus è un programma definito tramite il suo comportamento. Trasferisce codice/dati ad altri file di computer. Quando prende il controllo di questi altri file, si attiva in un qualche modo e cerca di infettare altri file. Questo processo viene definito replica. Un programma di computer viene chiamato "virus" quando è in grado di eseguire questo compito in modo ricorsivo.

Il Sandbox di Norman è un mondo virtuale in cui tutto viene simulato. È supportato da un emulatore e insieme consentono l'esecuzione di eseguibili binari potenzialmente infetti come se fossero in un sistema vero. Quando si interrompe l'esecuzione, il Sandbox viene analizzato per vedere cosa è cambiato.

Tecniche di sicurezza con Sandbox - macchina virtuale

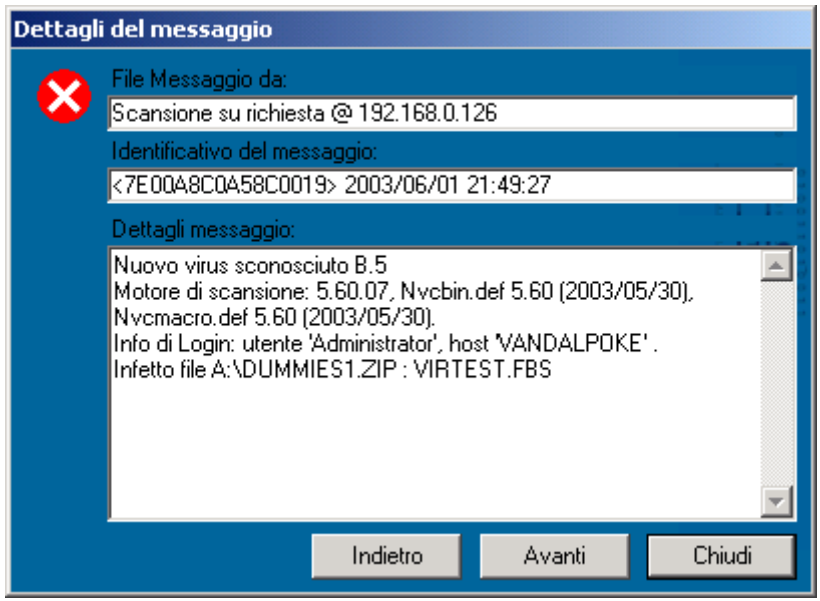
È anche possibile costruire un sandbox creando una macchina virtuale (VM, Virtual Machine). L'idea è bloccare tutte le uscite in modo tale da impedire la fuga all'eseguibile che si sta esaminando. Tuttavia questa soluzione non viene considerata sufficientemente sicura. Ci sarà sempre un "altro" exploit del processore del PC, interruzioni/eccezioni/guasti strani che consentono al codice dannoso di scappare dalla macchina virtuale e diffondersi nel sistema vero.

Quali sono i vantaggi per l'utente?

L'idea fondamentale della tecnologia Sandbox è offrire una migliore protezione agli utenti. L'obiettivo principale è integrare questa nuova tecnologia nel prodotto senza rallentare la velocità di scansione. L'altro problema capitale, quello dei falsi allarmi, è già stato risolto. La tecnologia Sandbox di Norman è stata introdotta ufficialmente in NVC v5.60, anche se era già utilizzata "di nascosto" dal motore di scansione da qualche tempo. A partire dalla versione 5.60 la tecnologia Sandbox è visibile tra le opzioni di configurazione di alcuni moduli.

Copyright © 1990-2005 Norman

Se viene rilevato del nuovo codice dannoso, l'amministratore viene informato con un messaggio simile a questo:



Visto che le tecniche avanzate impiegate in questo processo, il tempo di scansione aumenta leggermente quando è attiva l'opzione Sandbox. Tuttavia è un prezzo minimo da pagare se si considera il possibile guadagno derivante dal blocco di worm di rete, ad esempio.

Cosa fare quando Sandbox rileva un nuovo virus

Innanzitutto controllare che l'installazione di NVC sia aggiornata con i file di definizione dei virus più recenti. Se NVC non è aggiornato, Sandbox potrebbe aver trovato un virus che *ora* fa parte dei file di definizione.

Se si tratta di un nuovo virus, comprimere il file infetto, proteggere il file compresso con una password e inviarlo all'indirizzo *analysis@norman.no*. Questa procedura è descritta anche sul sito Web di Norman.

Per ulteriori informazioni sulla tecnologia Sandbox di Norman, consultare i white paper pubblicati in precedenza a questo riguardo. Sono disponibili nel sito web di Norman:

Copyright © 1990-2005 Norman

http://www.norman.com/documents/nvc5_sandbox_technology.pdf

http://www.norman.com/documents/nvc5_sandbox_technology_2002.pdf

Copyright © 1990-2005 Norman

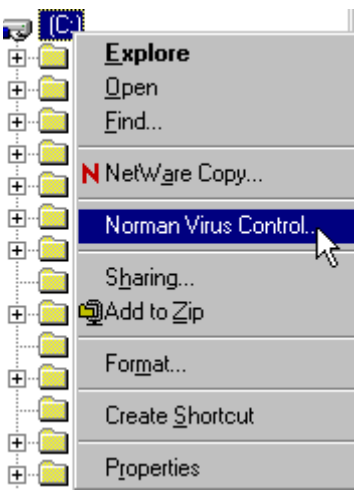
Domande frequenti (FAQ)

Se non trovate una risposta alle vostre domande nelle pagine seguiti, visitate il sito web per scaricare gli aggiornamenti. Questo elenco di domande frequenti (FAQ) verrà aggiornato su www.norman.com e nelle revisioni future di questo manuale.

Per noi è importante conoscere la vostra opinione su questo documento. Inviare i commenti e i suggerimenti per migliorare questo documento come pure in generale la documentazione scrivendo a documentation@norman.no.

Come si avvia NVC?

I componenti chiave di NVC si avviano automaticamente quando si carica il sistema operativo. Controllare che nella barra delle applicazioni appaia la piccola "N" verde di Norman.



Come si esegue una scansione alla ricerca di eventuali virus?

La scansione all'accesso è la funzione principale di controllo dei virus di NVC v5. Quando si accede un file, NVC controlla se contiene dei virus. Il "problema" è che la scansione all'avvio è invisibile. Se si desidera eseguire un controllo più tangibile, è possibile:

1. Evidenziare un qualsiasi oggetto del file system, ad esempio la lettera di unità (C:) in Esplora risorse.
2. Fare clic con il pulsante destro del mouse.
3. Dal menu selezionare "Norman Virus Control".
4. Fare clic sul pulsante **Analizza** per eseguire una scansione manuale di tutti i file presenti nelle unità o directory selezionate.

Avvio e interruzione della scansione all'accesso

Si consiglia di interrompere la scansione all'accesso quando si eseguono operazioni di manutenzione del sistema. Una volta interrotta, non si riavvierà nella sessione corrente o al riavvio successivo del sistema, a meno che non lo si faccia manualmente. È possibile interrompere e avviare la scansione

Copyright © 1990-2005 Norman

all'accesso da una voce di menu diversa (barra delle applicazioni) oppure dalla finestra di dialogo con schede **Avvio** nell'Editor di Configurazione (Norman Virus Control|Componenti|Avvio).

È necessario eseguire ogni giorno la scansione?

Non necessariamente. Se si abbinano delle scansioni periodiche su richiesta con delle scansioni programmate, la scansione all'accesso controlla che il PC non venga attaccato da codice dannoso. Tuttavia, se si effettuano di frequenti dei download da Internet, è consigliabile eseguire la scansione più spesso.

È possibile automatizzare la scansione dei virus?

Sì. Dal gruppo di programmi Norman, selezionare "Editor Operazioni" e specificare in quali aree analizzare e quando.

Come si aggiorna NVC?

Utilizzare il modulo "Internet Update" (IU) per aggiornare NVC. Per configurare IU, utilizzare la finestra di dialogo con schede **Internet** nell'Editor di Configurazione (**Installazione e aggiornamento dei prodotti**). Questa finestra di dialogo consente di decidere se IU deve aggiornare NVC su richiesta, quando si accede a Internet (a seconda del tipo di connessione) oppure da un server in una rete.

Come si installano gli aggiornamenti scaricati?

Se ne occupa NVC. Una volta che Internet Update ha scaricato un pacchetto con l'aggiornamento, NPM esegue automaticamente l'aggiornamento vero e proprio. Dopo l'aggiornamento, potrebbe essere necessario riavviare il computer.

Con che frequenza è necessario aggiornare NVC?

Si consiglia di eseguire Internet Update una volta al giorno. I siti web della Norman forniscono informazioni sui nuovi virus e in alcuni paesi è previsto l'invio di messaggi di posta elettronica e SMS per segnalare eventuali virus.

Se NVC rileva un virus, occorre segnalarlo alla Norman?

In genere no. NVC è in gradi di rimuovere la maggior parte dei virus. Per rimuovere il virus, seguire le istruzioni a video.

Copyright © 1990-2005 Norman

NVC in aggiunta ad altro software antivirus

“Dopo aver installato NVC in aggiunta a una soluzione antivirus di un altro fornitore, il computer si blocca completamente e ricevo molti messaggi di errore".

È probabile che i diversi prodotti antivirus siano in conflitto in quanto spesso tentano di analizzare gli stessi file contemporaneamente. Tutto ciò ha ripercussioni sulla stabilità del PC e crea comportamenti indesiderati.

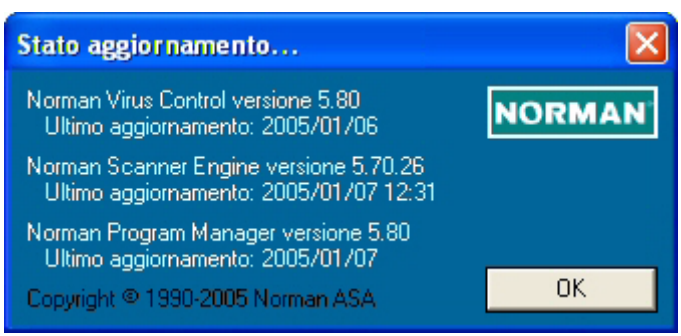
Consiglio: Disinstallare gli altri programmi antivirus prima di installare NVC.

Se questo problema si manifesta in Windows NT4, 2000 o XP, potrebbe essere necessario avviare il PC in modalità provvisoria prima di riuscire a disinstallare uno dei prodotti antivirus in conflitto. Per avviare il PC in modalità provvisoria, premere F8 all’avvio prima che venga caricato Windows.

NVC e i numeri di versione: come è possibile verificare se NVC è aggiornato?

Per individuare il numero di versione di NVC, scegliere **Stato aggiornamento** dal menu dell'icona sulla barra delle applicazioni (N).

Qui sono disponibili i numeri di versione per NVC, per il motore di scansione e il Program Manager. I file di definizione dei virus aggiornati frequentemente per i virus binary e delle macro si trovano all'interno del motore di scansione:



Norman Virus Control viene considerato aggiornato se le date di firma dei file di definizione dei virus non sono più vecchie di 10-12 giorni rispetto alla data corrente. Inoltre controllare che siano

Copyright © 1990-2005 Norman

stati scaricati e installati tutti gli aggiornamenti disponibili degli altri componenti di NVC.

Non preoccuparsi se il numero della versione del motore di scansione è diverso dal numero della versione corrente di NVC in quanto il motore di scansione ha un proprio numero di versione interno.

Copyright © 1990-2005 Norman

Indice

—A—

A intervalli definiti dall'utente 23
A intervalli predefiniti 23
Abbinamento dei diversi parametri 114
ACE 95
Aggiorna i file di configurazione da 25
Aggiorna il software da 25
Aggiorna server di distribuzione 29
Aggiornamento di NVC 21
Analizza file nuovi o modificati 66, 67
Analizza file prima del loro utilizzo 66
Analizza i file d'archivio 61
ARC 95
ARJ 95
autenticazione 30
Autostart: Minimizzata, visualizza solo se è rilevata l'infezione 96
Autostart: Minimizzata, visualizza solo se la pulizia fallisce 95
Autostart: Nascosta, visualizza solo se la pulizia fallisce 95
Avvio manuale: Finestra normale 96

—B—

barra delle applicazioni 14
Blocca allegati crittografati 83
Blocca estensioni CLSID 82
Blocca qualsiasi allegato con estensione doppia 82
Blocca tutti gli allegati elencati di seguito 83
Blocca tutti gli allegati, ad eccezione di quelli elencati di seguito 83
bloccare allegati (NIP) 81
Blocco degli allegati
    Blocca allegati crittografati 83
    Blocca estensioni CLSID 82
    Blocca qualsiasi allegato con estensione doppia 82
    Blocca tutti gli allegati elencati di seguito 83
    Blocca tutti gli allegati, ad eccezione di quelli elencati di seguito 83
    Block all attachments 82
    Elenco allegati 83
    Livello di sicurezza 84
    stringa 84
Block all attachments 82
BZIP2 95

—C—

cavalli di troia 78
Chiave di autenticazione per l'installazione/aggiornamento 20
Come agire in presenza di file che non possono essere analizzati 70
Comunità 49
Configurazione di NIP
    newsgroup (NNTP) 80
    NNTP 86
    POP 86
    posta in arrivo (POP3) 80
    posta in uscita (SMTP) 79
    SMTP 86
    Utilizza Sandbox 80
Configurazione di SMS
    Comunità 49
    Destinatari messaggio 47
    frequenza di baud 46
    Limite messaggio 47
    Modalità connessione 47
    Porta COM 46
    Testo comune SMS 48
connessione permanente 23
connessione via modem 24
Convenzioni iv
cracker di password 56, 68
Crea file di log 59
Credenziali di accesso 30
Credenziali di accesso al server proxy
    Dominio (per Windows NT chal-

Copyright © 1990-2005 Norman

lenge/response) 31
Nome utente 30
Password 31

—D—

default.ndf 77
Definizione
DLL 77
lettori di news 74
protocollo 74
Winsock 74
Dimensione massima quarantena (% partizione) 88
diritti 17, 70
diritti di amministratore 17, 70
Durata massima quarantena dei file 88
Durata minima quarantena dei file 88
Dynamic Link Library (DLL) 77

—E—

Editor di configurazione 12
Editor Operazioni 12, 51, 91
Analizza archivi 95
Analizza memoria 95
Analizza settori di boot 95
Analizza sottocartelle 94
Coordinate Tempo Universale 97
Data/ora di inizio: 97
Finestra di scansione 95
Finestra normale 96
Frequenza 97
Generale, scheda 92
Minimizzata, visualizza solo se è rilevata l'infezione 96
Minimizzata, visualizza solo se la pulizia fallisce 95
Nascosta, visualizza solo se la pulizia fallisce 95, 96
Operazione pianificata 96
Opzioni, scheda 95
Pianificazione, scheda 96
Seleziona target indipendenti dalla macchina 93
Seleziona unità e cartelle specifiche 94
Selezione dei target 93
Target, scheda 92
Tutte le unità di rete 94
Tutte le unità fisse 94
Tutte le unità rimovibili 94
Utilizzo risorse 96
Elementi aggiuntivi del percorso 25
e-mail 42
E-mail, SMS, SNMP
Errori di programma e di installazione 43
Impostazioni di default 43
Infezione da virus e altri allarmi 43
Errori di programma e di installazione
Routing messaggi 41
Escludi dalla scansione 57, 69
Esegui back up dei file da inviare in quarantena prima di ripararli 88
estensione doppia 82
estensioni CLSID 82

—F—

file di definizione dei virus 20
File di formato indefinito 57
file di log 35
da tenere 60
File di messaggio, scheda
Opzioni del Menu di scelta rapida 103
File elencati nella Lista di esclusione 58
File in quarantena
Opzioni del Menu di scelta rapida 100
File Operazione
File Operazione 99
Opzioni del Menu di scelta rapida 99
Programma 99
Prossimo avvio 99

Copyright © 1990-2005 Norman

Ultimo avvio 99
file Operazione pianificazione 99
File su unità di rete 58
Floating Point Unit (FPU) 12
Frequenza degli aggiornamenti su Internet 27
frequenza di baud 46

—G—

GZIP 95

—I—

Impostazioni comuni
Nuovi virus sconosciuti 57
Pubblicità invadente 57
Rischi di sicurezza 68
Indicazione dei percorsi
Aggiorna i file di configurazione da 25
Condivisione 25
Elementi aggiuntivi del percorso 25
Nome del server 25
Nome volume e directory principale 25
variabile di ambiente 26
Infezione da virus e altri allarmi
Routing messaggi 41
Inoltra messaggi 42
Installa, scheda
Chiave di autenticazione per l'installazione/aggiornamento 20
Installazione e aggiornamento del prodotto
Installa, scheda 19, 20
Lingua 20
Norman Scanner Engine 20
Norman Virus Control 19
Internet Update 12, 33, 52
NIU 104
Internet Update (IU) 26
Internet, scheda
Aggiorna server di distribuzione 29
Frequenza degli aggiornamenti su Internet 27
Logon al server proxy 30
Non utilizzare Internet – aggiorna da CD 27
Ogni giorno tramite connessione via modem (attendi connessione) 28
Server proxy 30
Solo su richiesta (avvia manualmente) 28
Tramite connessione diretta a orario programmato 28, 105
Utilizza un server proxy 30
Invia messaggi al file di log binario 35
Invia messaggi al Log degli eventi di Windows NT/2000 38
Invia messaggi alla console messaggi 37
IU 26
download dei pacchetti 107
Ogni giorno tramite connessione via modem (attendi connessione) 105
pacchetti 106
Solo su richiesta (avvia manualmente) 105

—L—

LAN/WAN
Automaticamente dal server 107
LAN/WAN, scheda
A intervalli definiti dall'utente 23
A intervalli predefiniti 23
Aggiorna i file Operazione da 25
Aggiorna il software da 25
Condivisione 24
Credenziali di accesso 30
Mai (aggiorna da CD o da Internet) 22
Nome server distribuzione 24

Copyright © 1990-2005 Norman

Nome volume e directory principale 24
Novell NetWare 24
Percorsi definiti dall'utente 24
Percorso degli aggiornamenti sulla LAN/WAN 24
Tipo di rete 24
Windows NT/2000/XP 24
Workgroup o rete peer-to-peer 24
lettori di news 74
limite messaggio 47
Linux iv
Logger messaggi
Errori di programma e di installazione 36
Infezione da virus e altri allarmi 36
Invia messaggi al file di log binario 35
Messaggi di attività di sistema e di rete 36
Messaggi di avvertimento 36
Messaggi generati localmente 35
Messaggi informativi 36
Messaggi ricevuti da altri computer 36
Logon al server proxy 30

—M—

macchina virtuale (VM) 118
Mai (aggiorna da CD o da Internet) 22
malware 71
Memoria, scansione 95
Messaggi
Campi presenti nella sezione Messaggi 102
Messaggi di attività di sistema e di rete
Routing messaggi 41
Messaggi informativi
Routing messaggi 41
Messaggi SMS 42
Messaggi, scheda
Data-Ora 102
Info 102
Messaggio 102
Opzioni del Menu di scelta rapida 102
Origine 102
Tipo 102
Minimizzata, visualizza solo se è rilevata l'infezione 96
Modalità connessione 47
Modem GSM 46
MSN Messenger 80
Multi Media Extensions (MME) 12

—N—

Nessun limite per gli allarmi 47
newsgroup (NNTP) 80
NIP
bloccare allegati specifici 85
bloccare tipi di file 84
blocco degli allegati 81
default.ndf 77
Numeri di porta 86
POP 86
NIP configuration
Instant Messaging 80
nip.exe 77
niphk.dll 77
NIUcf 26
niucf.exe 106
NNTP 77
NNTP (Network News Transfer Protocol) 86
Non utilizzare Internet – aggiorna da CD 27
Norman Internet Protection 52
Norman Internet Update
Impostazioni di configurazione 105
Norman Program Manager
Internet Update 33
Norman Internet Update 33
Note sulla versione 33
Supplemento a Messenger 33
Note sulla versione 33
Novell NetWare 24
numeri di porta 86

Copyright © 1990-2005 Norman

nuovi virus sconosciuti che utilizzano Sandbox 57

—O—

Ogni giorno all'atto della connessione del modem (attendi connessione) 27, 28
Ogni giorno con connessione diretta ad orario programmato 28
Ogni giorno tramite connessione via modem (attendi connessione) 28
Operazione pianificata 96
OS/2 iv

—P—

Parametri
abbinamento 114
Percorsi definiti dall'utente 24
Percorso degli aggiornamenti sulla LAN/WAN 24
Percorso file di log 59
Pianificatore Operazioni 51, 52
POP (Post Office Protocol) 86
POP3 77
Porta COM 46
Porta SMTP 44
posta in arrivo (POP3) 80
posta in uscita (SMTP) 79
Proprietà della quarantena 88
Protocollo
NNTP 74
POP3 74
SMTP 74
protocollo 74
proxy 30
Proxy HTTP 106
Pubblicità invadente 57, 68

—Q—

Quarantena
Opzioni 88
Quarantena, scheda
Esegui back up dei file da inviare in quarantena prima di ripararli 88
Sposta in quarantena i file irreparabili 88

—R—

RAR 95
Requisiti di sistema iv
Requisiti, sistema iv
Ricerca virus, cavalla di troia, worm, ecc. 67
rimozione dei virus 110
riparazione dei file 110
Rischi di sicurezza 56, 68
Rispondi alle chiamate di rete e abilita routing dei messaggi per:
Routing messaggi 40
Routing messaggi
Errori di programma e di installazione 41
Infezione da virus e altri allarmi 41
Messaggi di attività di sistema e di rete 41
Messaggi di avvertimento 41
Messaggi informativi 41
Messaggi ricevuti da altri computer 41
Rispondi alle chiamate di rete e abilita routing dei messaggi per: 40

—S—

sandbox 57, 68, 80
Scanner all'accesso
Rilevamento di nuovi virus sconosciuti mediante Sandbox 68
Scansione all'accesso 51
Analizza file nuovi o modificati 66
Analizza file prima del loro utilizzo 66
Chiedi all'utente 71

Copyright © 1990-2005 Norman

Come agire in presenza di file che non possono essere analizzati 70
Escludi dalla scansione 69
File di formato indefinito 69
File elencati nella Lista di esclusione 69
File su unità di rete 69
Ignora 70
Nega l'accesso 71
Pubblicità invadente 68
Rimozione dei virus 71
Rimuovi 71
Strategia 65
Utilizza modalità di scansione per servizi e utenti remoti 70
Visualizza messaggio 70
Visualizza messaggio e nega l'accesso 70
scansione all'accesso
Servizi terminal 89
Scansione all'accesso (utenti locali)
Analizza file nuovi o modificati 67
Analizza file prima del loro utilizzo 66
Strategia 66
scansione attivata mediante il pulsante destro del mouse 62
Scansione da linea di comando 51
scansione da linea di comando 109
Scansione su richiesta 50, 52
Analizza i file d'archivio 61
Crea file di log 59
Escludi dalla scansione 57
File di formato indefinito 57
File elencati nella Lista di esclusione 58
File su unità di rete 58
Log dettagliato 60
nuovi virus sconosciuti che utilizzano Sandbox 57
Pubblicità invadente 57
Ricerca 56
Rischi di sicurezza 56
Scansione attivata mediante il pulsante destro del mouse 62
Solo infezioni ed errori di log 60
scheda di avvio di NVC
Pianificatore Operazioni 52
Scansione all'accesso 52
scheda di installazione di NVC
Editor Operazioni 51
Norman Internet Protection 52
Pianificatore Operazioni 51
Scansione all'accesso 51
Scansione da linea di comando 51
Scansione su richiesta 50
Utilità 52
Seleziona target indipendenti dalla macchina 93
Seleziona unità e cartelle specifiche 94
Server proxy 30
Server SMTP 44
Service Provider SMS 47
servizi terminal 89
Servizi terminal di Windows NT/2000 89
SMTP 77
SMTP (Simple Mail Transport Protocol) 86
SNMP
Destinatari Trap 48
Solo su richiesta (avvia manualmente) 28
Sposta in quarantena i file irreparabili 88
strumenti di amministrazione remota 56, 68
Supplemento a Messenger 33

—T—

TAR 95
TCP/IP 104, 105
Tramite connessione diretta a orario programmato 28
Trap SNMP 42

Copyright © 1990-2005 Norman

—U—

UTC 97
Utilità 12, 52
    File di messaggio, scheda 103
    File Operazione 98
    Messaggi, scheda 101
    Quarantena, finestra di dialogo 100
Utilità, modulo 98
Utilizza Sandbox 80
Utilizza un server proxy 30
Utilizzo di Sandbox
    emulazione 118
    macchina virtuale 118
Utilizzo risorse 96

—V—

variabile di ambiente 26
virus crittografati 12
virus del settore di boot 62, 71, 110
virus polimorfici 12
visualizzare quarantena 100

—W—

Windows Messenger 80
Windows NT/2000/XP, rete 24
Winsock 74, 77
winsock.dll 74
Workgroup o rete peer-to-peer 24
worm di posta elettronica 57, 68, 81
worm di rete 57, 68, 81

—Z—

Zanda 108

Copyright © 1990-2005 Norman